

BELKIN®

Serieller OmniView® Konsolenserver





Benutzerhandbuch

F1DP116Sea



Table of Contents














Einleitung

Vielen Dank für den Kauf des seriellen OmniView Konsolenservers von Belkin. Dieses Gerät ermöglicht Administratoren die sichere Überwachung und Kontrolle von Servern, Routern, Switches und anderen seriellen Geräten über das TCP/IP-Unternehmensnetzwerk, Internet oder DFÜ-Modemverbindungen, selbst wenn der Server nicht im Netzwerk zur Verfügung steht.

Der Konsolenserver bietet Folgendes:

- Datenpfad-Sicherheit durch SSH oder Web/SSL
- Sichere, verschlüsselte Web-Oberfläche über SSL (HTTPS)
- SSHv2-Verschlüsselung für den sicheren Schutz von Zugangskennwörtern vor Hackern
- Unterstützung für alle gängigen SSH-Clients
- sicherer Zugriff über jeden Java-fähigen Browser
- Verbindung mit seriellen Konsolenanschlüssen über CAT5-Standardkabel, dadurch keine Probleme mit proprietären Kabelsystemen





Verpackungsinhalt

1 x serieller OmniView Konsolenserver

1 x Netzkabel

5 x Seriell/RJ45-Adaptersatz (5 Teile)

1 x Adapter Lokale Konsole/Serielle Schnittstelle

1 x RJ45/RJ45 CAT5-Kabel, 1,8 m

1 x Kurzanleitung

1 x Benutzerhandbuch auf CD

1 x Rack-Halterungen mit Befestigungsschrauben

1 x Gummimattensatz





Merkmale des Konsolenservers

- **In-Band- und Out-of-Band-Verwaltung**
  Die Konsolenschnittstellenverwaltung bietet zuverlässigen und sicheren Fernzugriff auf serielle Konsolenschnittstellen über In-Band-Netze und Out-of-Band-Verbindungsmöglichkeiten wie seriellen Terminalzugriff oder DFÜ-Modem.
- **Zentrale, sichere Fernverwaltung von Netzwerkgeräten/-servern**
  Die zuverlässige Konsolenschnittstellen-Verwaltung ermöglicht die Verschlüsselung sensibler Daten über bewährte Protokolle wie SSH/v2 und SSL.
- **Verwaltung für unterschiedliche Geräte**
  Eine einfache ASCII- oder VT-100-Terminalemulation ist zur Verwaltung eines breiten Spektrums von Gerätetypen nicht ausreichend. Moderne Datenzentren nutzen heterogene Gerätekombinationen aus UNIX-®, Linux-®, RISC-, Mainframe- und Windows-® Servern und anderen seriell verwalteten Geräten wie Routern, Gateways, Firewalls, Nebenstellenanlagen, USV, SAN- und NAS-Geräten sowie intelligenten Stromleisten.
- **Proaktive Überwachung und Warnfunktionen zur Unterstützung der Systemdiagnose**
  Anwendungen und Betriebssysteme senden Meldungen an die Systemkonsole. Sie enthalten Fehler- und Warninformationen, die oft einem Systemabsturz vorausgehen. Anders als Terminalserver speichern Konsolenschnittstellen-Server die Meldungen in Echtzeit. Administratoren können diese Daten auch später noch durchgehen und durchsuchen. Bei kritischen Ereignissen benachrichtigen Konsolenschnittstellen-Server den IT-Administrator verzögerungsfrei per E-Mail.



- **Entfernte, sichere Energiekontrolle**
  Über die serielle Schnittstelle fungiert dieses Gerät als Master zur Kontrolle von Stromleisten. Es können bis zu 15 Stromleisten angesteuert werden.
- **Seriell/Seriell-Funktion**
  Diese Funktion ermöglicht die Integration in einen Terminalkonverter, der lokal VGA- und Tastaturanschlüsse bereitstellt, oder die Verbindung der VGA/Tastaturschnittstellen mit einem KVM-Switch, der die Verwaltung in einem Gerät zusammenfasst.
- **Zugriffslisten für Benutzer**
  Durch Zugriffskontrolllisten für die Benutzerkontenverwaltung verfügen alle Benutzer mit Ausnahme der **admin** -Konten über eine bestimmte Reihe von seriellen Schnittstellen. Benutzer können die seriellen Schnittstellen ansteuern und konfigurieren, die von einem **admin** -Konto aus für sie freigegeben wurden.







Erforderliches Zubehör

- Universal-Anschlusssatz (enthalten)
- RJ45/RJ45-CAT5-Kabel (enthalten)

Systemvoraussetzungen

Web-Browser

Browser		
Betriebssystem	Microsoft Internet Explorer Version 6.0 SP1 und höher	Firefox Version 2.0 oder höher
Windows 2000 SP2	Ja	Ja
Windows Server 2003	Ja	Ja
Windows XP	Ja	Ja
Windows Vista	Ja	Ja
Red Hat Linux 3 und 4	Nein	Ja
Sun Solaris 9 und 10	Nein	Ja
Novell SUSE Linux 9 und 10	Nein	Ja
Fedora Core 4 und 5	Nein	Ja
Mac OS X 10.4+	Nein	Ja




Java-Plug-In
Für die Weboberfläche des Konsolenservers muss JRE (Java Runtime Environment) 6.0 oder höher installiert sein. Die aktuelle Java-Software erhalten Sie auf der Website: http://www.java.com/en/download/manual.jsp.





Bestandteile

Vorder-/Rückseite

Abb. 1 Vorderansicht

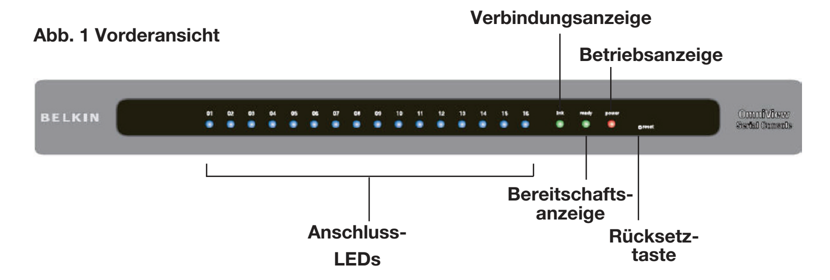
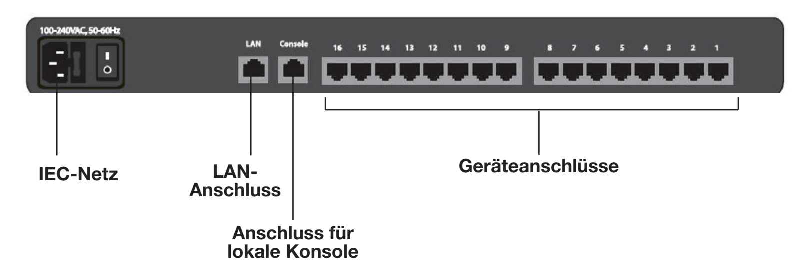


Abb. 2 Rückansicht



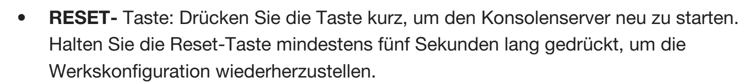






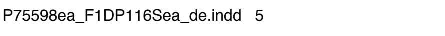

LED-Anzeigen, Taste und Anschlüsse

LED	Bedeutung
Power (Ein/Aus)	**Rot –** Stromversorgungsanzeige *AN: Gerät wird mit Strom versorgt*
Link (Verbindung)	**Ethernet-Verbindung/Aktiv/10/100Mbit/s:** **Orange –** 10BaseT Ethernet-Verbindung ist hergestellt **Grün –** 100BaseT Ethernet-Verbindung ist hergestellt *Blinkanzeige: Bei Datenaktivität* *AN: Wenn keine Datenaktivität besteht und Verbindung hergestellt ist*
Betriebsbereit	**Grün** – Blinkt jede Sekunde, wenn das System betriebsbereit ist
Schnittstellenak-tivität (eine LED-An-zeige je Port)	**Blau** – Datenverkehr *AN: In Verwendung (erfolgreiche Anmeldung an der Schnittstelle)* *Blinkanzeige: Datenverkehr an der seriellen Schnittstelle*





- **RESET-** Taste: Drücken Sie die Taste kurz, um den Konsolenserver neu zu starten. Halten Sie die Reset-Taste mindestens fünf Sekunden lang gedrückt, um die Werkskonfiguration wiederherzustellen.
- **ETHERNET** RJ45 -Anschluss: Ethernet-Schnittstelle
- **CONSOLE** RJ45 -Anschluss: Lokale RS232-Konsolenschnittstelle
- **Weitere** RJ45 -Anschlüsse: serielle Schnittstellen





Technische Daten

Merkmale und Funktionen	Technische Daten
Allgemeine Merkmale	**LED-Anzeigen** Betrieb (rot) Bereit (grün, blinkt normalerweise auf), Verbindung/Aktiv/10/100Mbit/s (Ethernet orange: 10 Mbit/s, grün: 100 Mbit/s)
	Aktivität (blau für jeweilige serielle Schnittstelle)
	Taste zum Zurücksetzen oder Wiederherstellen der Werkseinstellung
	RTC (Echtzeituhr)
Serielle Schnittstelle	16-Port (F1DP116S)
	Serieller Schnittstellenbetrieb (RS232)
	Serieller Anschluss (RJ45)
	Baudrate (300 bis 115200)
	Flusskontrolle (keine, RTS/CTS, XEin/XAus)
LAN-Schnittstelle	RJ45-Anschluss
	IEEE 802.3 - 10/100BaseT
	Automat. Erkennung, Voll-/Halbduplex wählbar
Schnittstellenfunktion	**Betriebsmodi**
	Konsolenserver
	Terminalserver
	DFÜ-Modem
	Seriell/seriell (nur für Schnittstelle 16)
Protokolle	TCP, UDP, IP, ARP, ICMP, HTTP/HTTPS, Telnet, DHCP/BOOTP, PPP,
	SMTP, DNS, NTP
	Dynamisches DNS
Protokollbezogene Funktion	TCP-Nichtbedienungszeit (TCP-Aufrechterhaltung)
	Serielle Nichtbedienungszeit
	Schnittstellenüberwachung
Sicherheit	Kennwortzugriff
	IP-Filter
	SSHv2
	HTTPS/SSL
Authentifizierung	Lokale Benutzerdatenbank
	PAP/CHAP (für Modem-Einwahl)
	RADIUS
Bedienung	Lokale Konsole (Menü oder Befehlszeile)
	SSH, Telnet
	Webseiten (HTTP/HTTPS)
	Firmware-Upgrade über Web-Oberfläche
	Port-Überwachung und -Protokollierung
	Systemstatusfunktionen mit komfortablen Funktionen
Stromversorgung und Umgebung	Netzeingang (100 ~ 240 V AC, 50 ~ 60 Hz)
	Betriebstemperatur: -10° bis 80° C
	Lagertemperatur: -20° bis 85° C
	Relative Luftfeuchtigkeit: 0-90%, nicht kondensierend
Zulassungen	CE, FCC
	UL
Abmessungen und Gewicht	1 HE 19˝ Rackmount
	Abmessungen (cm): 43,2 x 18,0 x 4,2




Hinweis: Unangekündigte technische Änderungen jederzeit vorbehalten.





Aufstellungsort:

Der Konsolenserver kann wahlweise als eigenständige Desktop-Einheit verwendet oder in einem Rack befestigt werden. Er kann mit den beiliegenden Schrauben und Halterungen in einem Standard-Serverrack (19") befestigt werden.

Bitte beachten Sie bei der Aufstellung des Konsolenservers folgendes:

- Den Abstand zwischen den Zielgeräten und der Konsole
- Die Länge der Verbindungskabel zwischen Geräten und Konsole
- Die Stromquelle: Gerät darf nur an die auf dem Gerät angegebene Stromquelle angeschlossen werden. Beim Anschließen von mehreren, in einem Rack installierten elektrischen Komponenten ist darauf zu achten, dass die Gesamtgeräteleistung nicht über der Netzbelastbarkeit liegt.

Zulässige Kabellängen (für CAT5)

Bei seriellen Binärdatensignalen (RS232) sind aus Gründen der Übertragungsqualität Kabellängen von höchstens 15 m ratsam. Bei größeren Kabellängen kann sich die Signalqualität verschlechtern. Daher empfehlen wir für die Verbindung zwischen dem Konsolenservern und den Servern CAT5-UTP-Kabel von höchstens 15 m.




Kabel und Adapter

Belkin empfiehlt die Verwendung von CAT5, FastCAT5e oder CAT6-Patchkabeln von Belkin für Ihren Konsolenserver, damit die beste Signalqualität erzielt werden kann.

Belkin UTP-Patchkabel:

A3L791-XX-YYY (CAT5e)

A3L850-XX-YYY (FastCAT™ 5e)

A3L980-XX-YYY (CAT6)

Informationen zur Kontaktbelegung finden Sie in Anhang B auf Seite 54.

Belkin Seriell-Adapter:

F1D120ea (RJ45-Buchse–DB9-Buchse DTE)

F1D121ea (RJ45-Buchse–DB25-Buchse DTE)

F1D122ea (RJ45-Buchse–DB25-Stecker DCE)

F1D123ea (RJ45-Buchse–DB25-Stecker DTE)

F1D124ea (RJ45-Buchse–RJ45-Stecker CISCO)

F1D120ea-8PK (8er-Satz F1D120ea)

F1D124ea-8PK (8er-Satz F1D124ea)

Detaillierte Abbildungen der einzelnen Adapter finden Sie in Anlage A auf Seite 51.



Aufstellung auf dem Schreibtisch oder Befestigung im Rack

Der Konsolenserver kann auf dem Schreibtisch aufgestellt oder in einem 19-Zoll-Rack (1 HE) montiert werden.

Hinweis: Bevor Sie beginnen, notieren Sie die MAC-Adresse und die Seriennummer des Konsolenservers. Diese befinden Sie auf der Rückseite der Geräts. Sie benötigen diese Nummern ggf. während des Installationsvorgangs. Es ist daher wichtig, sich diese Nummern vor dem Einbau in das Rack zu notieren.

MAC-Adresse	Seriennummer

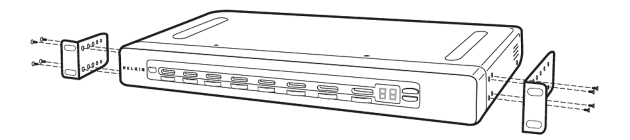
Der Konsolenserver enthält einstellbare Halterungen für den Einbau in ein 19"-Rack. Die Halterungen ermöglichen die Einstellung von drei Befestigungspositionen, sodass Sie die Vorderseite des Konsolenservers so anbringen können, dass er entweder bündig zu den Schienen abschließt oder über die Vorderseite der Schienen herausragt. Mit den folgenden einfachen Schritten erzielen Sie die gewünschte Einstellung.

Rack-Montage

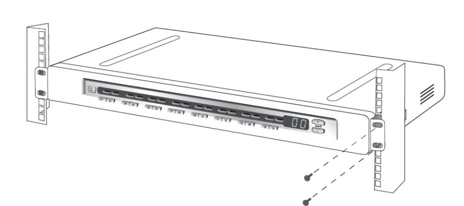
1 Überlegen Sie sich, wie weit der Konsolenserver über das Rack hinausragen soll. Wählen Sie die entsprechende Bohrungsanordnung für die Halterungen aus.




2 Befestigen Sie die Halterung mit den beigefügten Kreuzschlitzschrauben seitlich am Konsolenserver. (Siehe Abbildung unten.)



3. Montieren Sie den Konsolenserver mit den Schrauben an den Rack-Schienen. (Siehe Abbildung unten.)





Ihr Konsolenserver ist jetzt sicher im Rack befestigt und Sie können die Zielgeräte anschließen.

Anschließen der Zielgeräte an den Konsolenserver

1. Schalten Sie die Zielgeräte, die an den Konsolenserver angeschlossen werden sollen, ab.
2. Schließen Sie das Ethernet-Kabel an den Anschluss „LAN" an.
3. Schließen Sie das mitgelieferte Netzkabel an den Stromanschluss des Konsolenservers an. Schließen Sie das andere Kabelende an eine geeignete Steckdose an.

Hinweis: Warten Sie, bis der Konsolenserver hochgefahren ist (ca. 100 Sekunden).

4. Wählen Sie einen freien nummerierten Anschluss an der Rückseite des Konsolenservers aus. Schließen Sie daran ein UTP-Patch-Kabel an (4-paarig, bis zu 15 m). Schließen Sie das andere Kabelende an ein Zielgerät an. Verwenden Sie zum Anschluss an das Zielgerät nötigenfalls einen geeigneten Adapter. Weitere Informationen hierzu finden Sie in Anhang A auf Seite 51.
5. Wiederholen Sie diesen Vorgang für alle Zielgeräte. (Siehe Abbildung unten.)



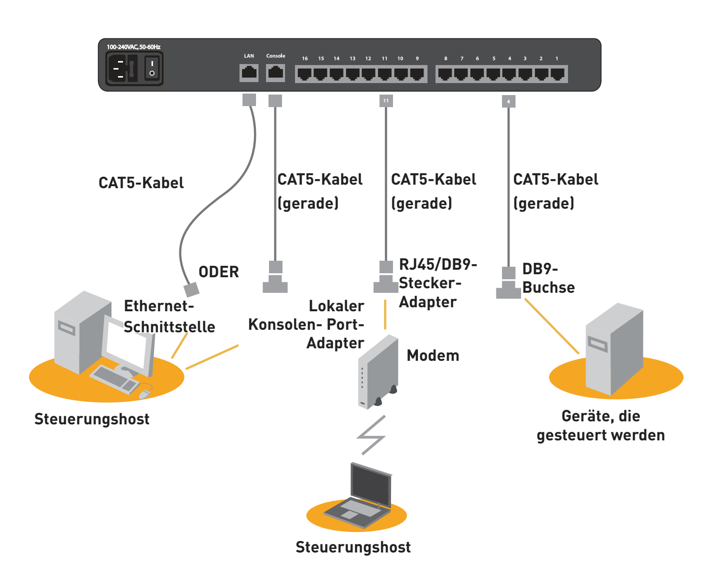


Abb. 3 Verkabelung: Kabelverbindungen für unterschiedliche Schnittstellen.





Bevor Sie die Verbindung zu einem Zielgerät herstellen können, müssen Sie die Netzwerkeinstellungen konfigurieren. Der Konsolenserver bietet zwei Möglichkeiten zur Einrichtung des Netzwerks an: über eine Browser-Oberfläche und über den lokalen Konsolenanschluss.

Der Konsolenserver unterstützt sowohl das Protokoll DHCP als auch die Zuweisung einer statischen IP-Adresse. Wir empfehlen, eine IP-Adresse für den Konsolenserver zu reservieren, die während der Verbindung zum Netzwerk statisch bleibt.

Browser-Oberfläche

Die Web-Oberfläche bietet eine einfache Möglichkeit zur Konfiguration des Konsolenservers. Der Administrator kann alle Merkmale über den Browser einstellen.

Anfangseinstellungen

Im folgenden Kapitel finden Sie Anweisungen für die Einstellung der IP-Adresse für den OmniView Konsolenserver.

Schritt 1: Erkennung der IP-Adresse

Wenn Ihr Konsolenserver in das Netzwerk eingebunden wurde und angeschaltet ist, wird dem Konsolenserver von einem DHCP-Server (Dynamic Host Configuration Protocol) in Ihrem Netzwerk automatisch eine IP-Adresse, eine Gateway-Adresse und eine Subnetz-Maske zugeteilt.



Um diese IP-Adresse in Ihren Netzwerk zu erkennen, verwenden Sie die MAC-Adresse an der Rückseite des Konsolenservers. Wenn in Ihrem Netzwerk kein DHCP-Server gefunden werden konnte, wird der Konsolenserver mit der folgenden statischen IP-Adresse gestartet: 192.168.2.156.

Wenn Sie mehrere Konsolenserver mit demselben Netzwerk verbinden möchten und kein DHCP-Server verfügbar ist, verbinden Sie jeden Konsolenserver nacheinander mit Ihrem Netzwerk und ändern Sie für jeden die statische IP-Adresse, bevor Sie die nächste Einheit einbinden.

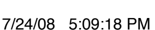
Hinweis: Wenn später ein DHCP-Server in Ihr Netzwerk eingebunden wird, erhält der Konsolenserver von diesem Server eine neue IP-Adresse. Um die ursprüngliche statische IP-Adresse zu erhalten, müssen Sie DHCP deaktivieren (siehe Seite 18).

Schritt 2: Anmeldung an der Web-Oberfläche

Nach der Bestimmung der IP-Adresse für Ihr Gerät öffnen Sie Ihren Web-Browser. Die Liste der unterstützten Browser finden Sie auf Seite 3.

Geben Sie die IP-Adresse des Konsolenservers folgendermaßen in das Adressfeld des Browsers ein: http://XXX.XXX.XXX.XXX (Beispiel: http://76.255.43.173). Die Anmeldeseite wird geöffnet (siehe nächste Seite). Fügen Sie diese Seite zu Ihren Lesezeichen hinzu, um sie später leichter aufrufen zu können.





Hinweis: Für die Kommunikation über eine SSL-Verbindung (Encrypted secure socket layer) kann HTTPS verwendet werden. Wenn Sie diese Seite zum ersten Mal öffnen, können zwei Sicherheitsmeldungen des Browsers angezeigt werden. Bestätigen Sie beide Warnungen mit „Ja".

Anmeldeseite

Geben Sie den folgenden Standard-Benutzernamen und das Kennwort ein. Achten Sie dabei auf Groß- und Kleinschreibung:



Benutzername	Kennwort
admin	admin



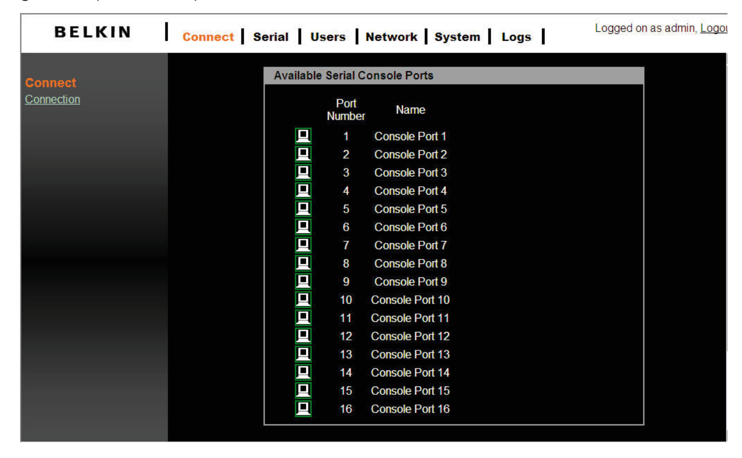
Für die Zugriffsrechte werden zwei Stufen angeboten:

Benutzername	Standard-Kennwort	Zugriffsrechte
admin	admin	Admin.-Zugriff
(Benutzername)	(Benutzername)	Nur Zugriff auf „Serial Port" (Serielle Schnittstelle) und „System Status" (Systemstatus)

Der Administrator kann einen Benutzer über die Webseiten der Systemverwaltung einfach und problemlos hinzufügen oder entfernen.



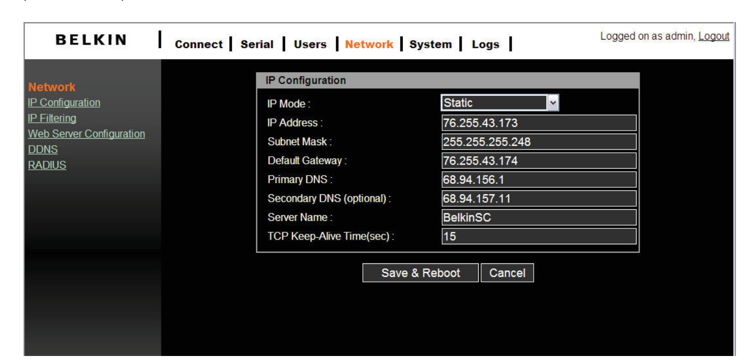
Klicken Sie Anmelden. Die Web-Oberfläche wird mit der Netzwerk-Verbindungsseite geöffnet (siehe unten).



Haupt-Verbindungsseite

Schritt 3 Netzwerkkonfiguration

Klicken Sie auf „Network" (Netzwerk), um die Netzwerk-Konfigurationsseite zu öffnen (siehe unten).



Netzwerkkonfigurationsseite

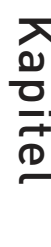
Hier können Sie eine statische IP-Nummer und weitere Netzwerkeinstellungen zuweisen.

Klicken Sie auf „Save & Reboot" (Speichern und Neustart), um die Einstellungen der Netzwerkkonfiguration zu speichern.

Hinweis: Wenn der Benutzer den Browser mehr als **30 Minuten** lang nicht betätigt, wird der Benutzer abgemeldet und die Sitzung beendet.







Zuweisen der IP-Adresse über die Konsolenschnittstelle VT-100 (Konsole, Telnet, SSH)

Der Konsolenserver bietet auch eine benutzerfreundliche, menügesteuerte Befehlszeilenoberfläche. Sie können einfach ein VT-100-Terminal an den lokalen Konsolenanschluss anschließen und damit auf den Konsolenserver zugreifen. Dies ist sinnvoll, wenn Sie die Netzwerkeinstellungen des Konsolenservers nicht kennen und nicht auf den Server zugreifen können. Über den lokalen Konsolenanschluss können Sie die Einstellungen (IP-Adresse, Subnetzmaske usw.) anzeigen und bearbeiten.

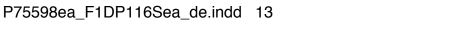
1. Verbinden Sie den Konsolenanschluss an der Geräterückseite mit Hilfe des CAT5-Kabels und des lokalen Konsolenanschlussadapters (RJ45/DB9-Buchse), im Lieferumfang des Belkin Konsolenservers enthalten) mit einer seriellen Schnittstelle an einem PC-Host.
2. Konfigurieren Sie ein Terminal-Emulationsprogramm wie HyperTerminal mit den folgenden Parametern:
    - Baudrate = 115200
    - Datenbits = 8
    - Stoppbits = 1
    - Parität: keine
    - Flusskontrolle = keine



```
+--------------------------------------------------------------+
|                  Belkin OmniView Serial Console              |
|              Copyright (c) 2007, All Rights Reserved         |
+--------------------------------------------------------------+
|                            Log In                            |
+--------------------------------------------------------------+

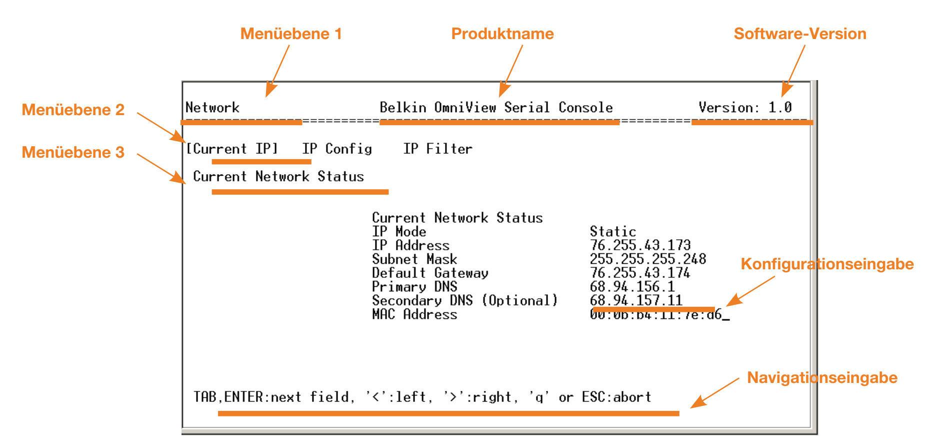
username : _
```

Hinweis: Die Benutzernamen und Kennwörter wurden über die Weboberfläche eingestellt und gelten auch hier unverändert. Der Standard lautet „admin/admin".

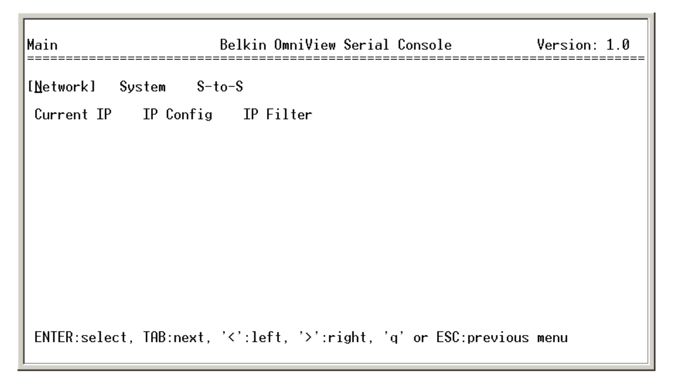




Die folgende Abbildung zeigt den Aufbau der Oberfläche.





Menü-Layout



Kapitel

1
2
3
4
5
6

7

8


Netzwerk > IP-Konfiguration

Die Seite links zeigt die IP-Konfigurationselemente.

1. Für den **IP-Betrieb** : Mit der Leertaste können Sie zwischen Statikbetrieb und DHCP-Betrieb wählen.
2. Für **IP-Adresse, Subnetz-Maske, Standard-Gateway, primäre und sekundäre DNS-Adresse** : Sie können diese Netzwerkeinstellungen bearbeiten.
3. Wenn Sie die Einstellungen bearbeitet und die Eingabetaste gedrückt haben, fordert der Konsolenserver Sie auf, diese mit YES zu bestätigen oder mit NO abzulehnen. Wählen Sie YES, führt der Konsolenserver einen Neustart durch und speichert die Einstellungen im Flash-Speicher.

Network > Current IP (Netzwerk > Aktuelle IP)

Zeigt die aktuellen Netzwerkeinstellungen an.

Network > IP Filter (Netzwerk > IP-Filter)

Aktiviert/deaktiviert die IP-Filterfunktion.

System > Reboot (System > Neustart)

Startet den Konsolenserver neu.

System > Reset to Default (System > Auf Werkseinstellung zurücksetzen)

Setzt die Konfiguration auf die Werkseinstellungen zurück.

Hinweis: Nur der Benutzer **admin** ist berechtigt, diese Funktion aufzurufen.

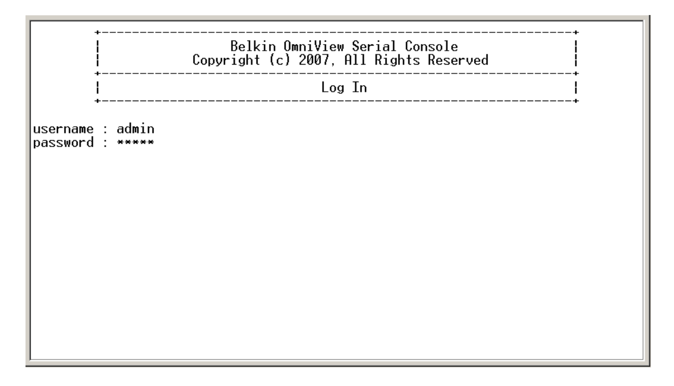
System > Status (System > Status)

Zeigt den Systemstatus an.

S-to-S > Select Serial-to-Serial Port (S-zu-S > Seriell/Seriell-Anschluss wählen)

Aktiviert die Seriell-/Seriellanschluss-Verbindung über Schnittstelle 16. Weitere Informationen finden Sie im Abschnitt „Seriell/Seriell-Funktion" auf Seite 34.





Hinweis:
Nur der Benutzer **admin** ist zur Anmeldung an VT-100 berechtigt. Alle anderen Benutzer können keine Konfiguration über VT-100 vornehmen.



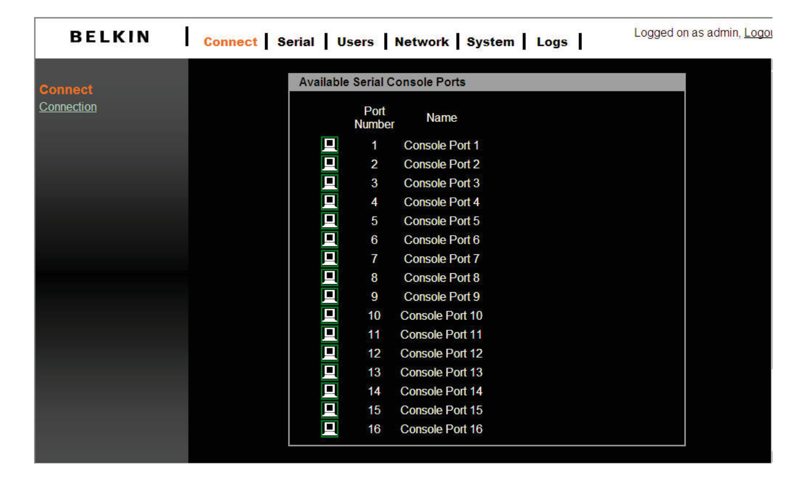

Browser-Verwaltungsoberfläche

Der Konsolenserver unterstützt sowohl das Protokoll HTTP als auch HTTPS (HTTP über SSL). Die Benutzer müssen sich durch die Anmeldung an das System mit einem korrekten Benutzernamen und Kennwort ausweisen.

Geben Sie zum Zugriff auf die Webverwaltungsseiten des Konsolenservers die IP-Adresse oder den Hostnamen in das Adressfeld des Browsers ein. Dadurch werden Sie automatisch mit dem Anmeldefenster verbunden.

Die Abbildung auf der nächsten Seite zeigt die Startseite der webbasierten Verwaltungsoberfläche. Am oberen Bildschirmrand befindet sich eine Menüleiste.
Das Untermenü wird links auf der Seite angezeigt und ermöglicht die Bearbeitung der Parametereinstellungen für das ausgewählte Hauptmenüelement.





Auf dieser Seite können verfügbare Aktionen übernommen oder abgebrochen werden. Um alle Änderungen zu übernehmen, wählen Sie „Apply" (Übernehmen). Die neuen Werte werden in die Konfiguration übernommen. Wenn Sie die neuen Werte nicht speichern möchten, klicken Sie auf „Cancel" (Abbrechen). Alle Änderungen werden dann aufgehoben und die vorherigen Werte wiederhergestellt.



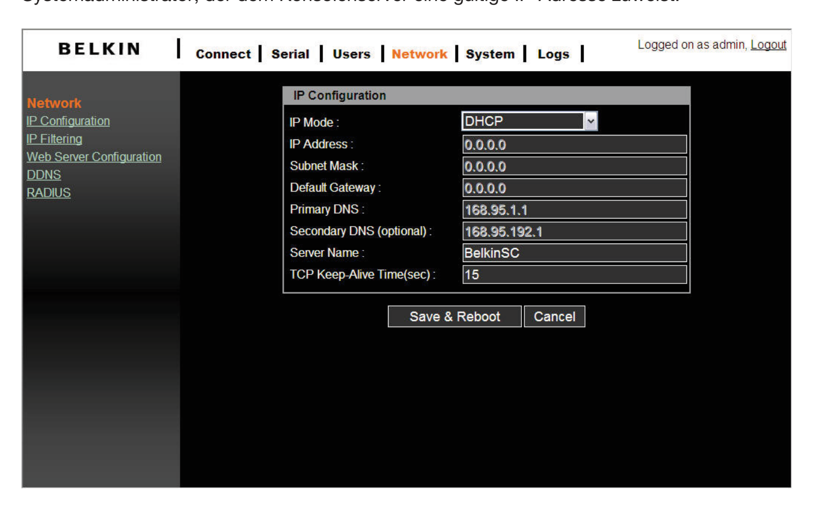





Sie können die Netzwerk-IP-Einstellungen über via VT-100 oder die Web-Oberfläche konfigurieren. In diesem Abschnitt wird die Konfiguration über die Web-Oberfläche beschrieben.

IP-Einstellungen

Der Konsolenserver benötigt für den Betrieb in der Netzwerkumgebung dese Benutzers eine gültige IP-Adresse. Wenn die IP-Adresse noch nicht bereitsteht, wenden Sie sich an den Systemadministrator, der dem Konsolenserver eine gültige IP-Adresse zuweist.






Zur Auswahl stehen zwei IP-Zuweisungsverfahren:

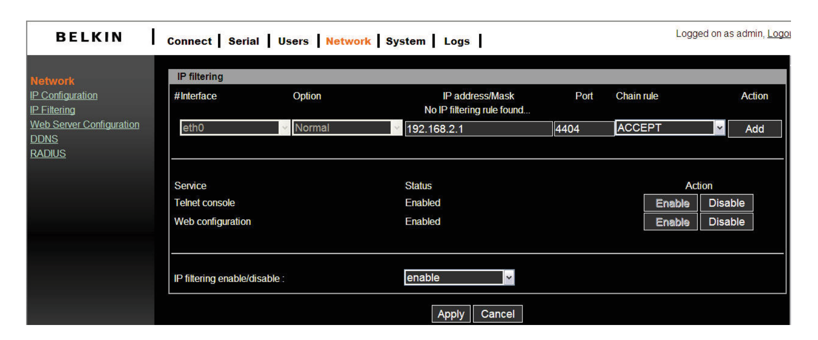
- Statische IP-Adresse
- DHCP (Dynamic Host Configuration Protocol).

Standardmäßig ist DHCP eingestellt. Wenn in Ihrem Netzwerk kein DHCP-Server gefunden werden konnte, wird der Konsolenserver mit der folgenden statischen IP-Adresse gestartet: 192.168.2.156.

Sie können die neue IP-Konfigurationseinstellung mit „Save & Reboot" (Speichern und neu starten) speichern.

IP-Filter

Der IP-Filter unterbindet mit Hilfe von Filterregeln den Zugriff durch nicht autorisierte Hosts auf den Konsolenserver.



Die IP-Adresse/-Maske legt den Hostbereich fest. Hierzu wird die IP-Adresse des Basis-Hosts eingegeben, danach ein "/" und die Subnetzmaske eingegeben. ("/" wird als Trennzeichen zwischen IP-Adresse und Subnetzmaske benötigt). Die Host-IP-Adressen werden anhand der definierten Regel gefiltert.

Nachstehende Tabelle zeigt Beispiele für IP-Adress- und Maskeneinstellungen.

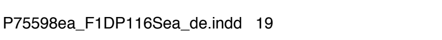
Festgelegter Hostbereich	Basis-Host IP-Adresse	Subnetz-Maske
Beliebiger Host	0.0.0.0	0.0.0.0
192.168.2.120	192.168.2.120	255.255.255.255
192.168.2.1 ~ 192.168.2.254	192.168.2.0	255.255.255.0
192.168.0.1 ~ 192.168.255.254	192.168.0.0	255.255.0.0
192.168.2.1 ~ 192.168.1.126	192.168.2.0	255.255.255.128
192.168.2.129 ~ 192.168.2.254	192.168.2.128	255.255.255.128

Der „Port" ist eine Schnittstelle oder ein Schnittstellenbereich des Konsolenservers, auf den die Hosts versuchen, zuzugreifen.

Kettenregel

Die Kettenregel bestimmt, ob der Zugriff durch die Hosts zugelassen wird. Sie kann einen von zwei Werten annehmen:

- **ACCEPT:** Zugriff zugelassen
- **DROP:** Zugriff nicht zugelassen





Wenn der Konsolenserver ein TCP-Paket empfängt, verarbeitet er es anhand der unten gezeigten Kettenregel. Die Verarbeitungsfolge ist wichtig: das Paket wird zunächst der Kettenregel 1 unterzogen. Erfüllt es die Regel, wird eine Aktion eingeleitet; andernfalls wird Kettenregel 2 abgearbeitet.

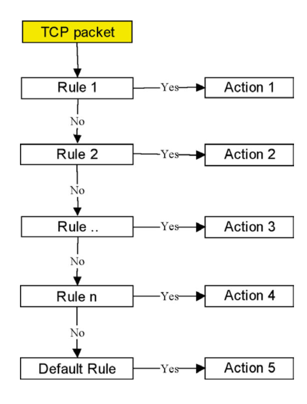
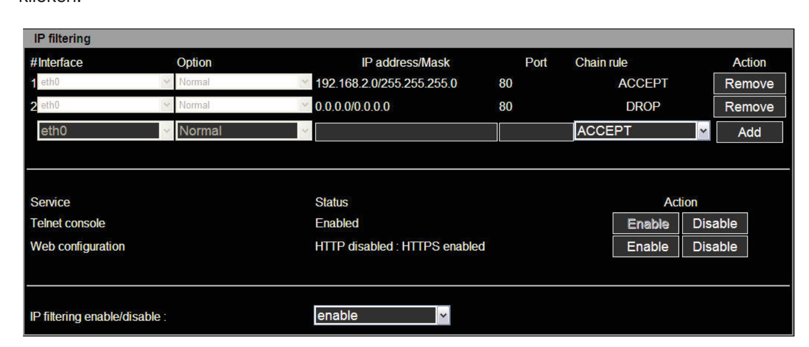


Abb. 4 Kettenregel für IP-Filter





Sie können eine neue IP-Filterregel hinzufügen, indem Sie die Eigenschaften in der nächsten leeren Eingabezeile eingeben. Klicken Sie nach der Eingabe auf „Add" (Hinzufügen), um die Aktion zu speichern. Sie können eine Regel entfernen, indem Sie auf „Remove" (Entfernen) klicken.



Im nachstehenden Beispiel werden die Regeln in der folgenden Reihenfolge angewendet:

Nr. 1. Hosts, die zum Subnetz 192.168.2.x gehören, wird der Zugriff auf den Konsolenserver (über http port 80) gestattet.

Nr. 2. Allen Hosts wird der Zugriff auf den Konsolenserver (über http port 80) verweigert.



Nach der Anwendung dieser Regeln können nur die Hosts des Subnetzes 192.168.2.x auf den Konsolenserver (über http port 80) zugreifen.

Zusätzlich zur vorstehend beschriebenen IP-Filterregel bietet die Web-Oberfläche eine bequeme Möglichkeit zur Aktivierung bzw. Deaktivierung von Telnet (Schnittstelle 23) oder der Web-Konfigurationsschnittstelle (Schnittstelle 80/443). Diese Dienste dienen hauptsächlich zur Konfiguration des Konsolenservers. Wenn Sie im Feld „Action" (Aktion) auf „Enable/Disable" (Aktivieren/Deaktivieren) klicken, können Sie Kettenregeln schnell und einfach hinzufügen oder abändern, ohne eine manuelle Bearbeitung vorzunehmen.

Hinweis:
Für eine bessere Textausrichtung sollte ein VT-100-kompatibler Telnet-Client verwendet werden. PuTTY ist einer der empfohlenen Telnet-Clients, die eine bessere Textausrichtung der Benutzeroberfläche bieten. Er kann auf der folgenden Website heruntergeladen werden

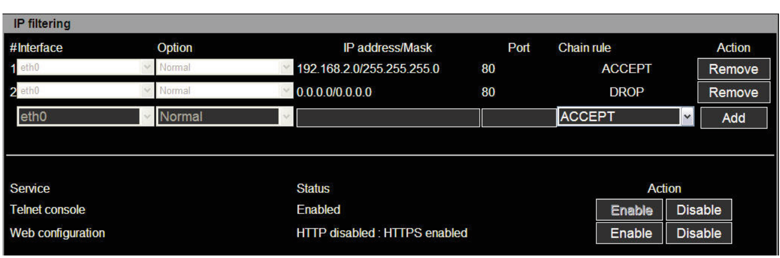
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

Webserver-Konfiguration

Der Webserver des Konsolenservers unterstützt die Protokolle HTTP und HTTPS (HTTP über SSL) gleichzeitig.
Sie können die Benutzer-Authentifizierungsmethode für die Web-Anmeldung auswählen. Der Konsolenserver bietet derzeit die Authentifizierungsmethoden Lokal und RADIUS.

Lokal

Der Konsolenserver verweist zur Benutzeranmeldung an den Webserver standardmäßig auf die lokale Datenbank.



RADIUS und Lokal

Der Konsolenserver verweist zur Authentifizierung des Benutzerkontos zuerst auf den RADIUS-Server. Wenn das Benutzerkonto nicht gefunden wird oder der RADIUS-Server abgeschaltet ist, sucht der Konsolenserver in seiner lokalen Datenbank nach dem Benutzerkonto. Das Gerät verweigert die Anmeldung, wenn der Benutzer weder in der RADIUS- noch on der lokalen Datenbank gefunden wird. Die RADIUS-Server kann benutzerseitig über die Konfigurationsseite des RADIUS-Servers konfiguriert werden. Weitere Angaben, siehe Seite 24.



Dynamisches DNS

Wenn ein Benutzer den Konsolenserver mit einer DSL-Leitung verbindet oder über eine DHCP-Konfiguration eine dynamische IP-Adresse aus dem Netzwerk bezieht, kann sich die IP-Adresse ändern. Dies kann es schwierig machen, festzustellen, ob sich eine IP-Adresse geändert hat oder wie die neue IP-Adresse lautet.

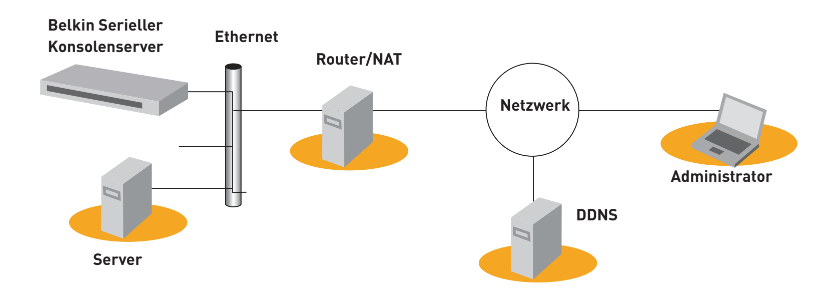


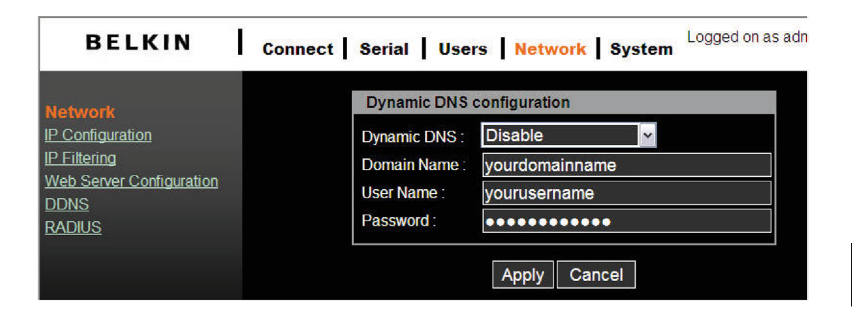
Abb. 5 Dynamisches DNS




Der Dynamische DNS-Dienst wird von zahlreichen Internet-Providern und Organisationen angeboten, um dieses Problem anzugehen. Über einen dynamischen DNS-Dienst können Sie anhand des Hostnamens, der im dynamischen DNS-Server gespeichert ist, auf den Konsolenserver zugreifen und sind somit unabhängig von IP-Adressenänderungen. Standardmäßig unterstützt der Konsolenserver nur den dynamischen DNS-Dienst von Dynamic DNS Network Services, LLC (www.dyndns.org).

Um den dynamischen DNS-Dienst von Dynamic DNS Network Services zu nutzen, müssen Sie ein Mitgliedskonto im NIC (Network Information Center - http://members.dyndns.org) eröffnen. Sie können dann einen neuen DNS-Hostlink hinzufügen, nachdem Sie sich an das entsprechende Mitglieder-NIC anmelden.

Nach dem Aktivieren des dynamischen DNS-Dienstes im Menü „Dynamic DNS Configuration" (Dynamische DNS-Konfiguration) müssen Sie den registrierten Domänennamen, Benutzernamen und das Kennwort eingeben. Nach der Übernahme der Konfigurationsänderung können Sie sich allein mit dem Domänennamen an den Konsolenserver anmelden. Das DNS (Domain Name Systems) ist Internet-Dienst, der Domänennamen in IP-Adressen auflöst.



Hinweis:
Im Feld Domänenname muss ein geeigneter Domänenname (Qualified Domain Name: FQDN) anstelle eines registrierten Hostnamens eingegeben werden.

RADIUS

Durch die so genannte Authentifizierung wird eine Person, meist über Benutzername und Kennwort, identifiziert. Der Konsolenserver unterstützt verschiedene Authentifizierungsoptionen wie „Lokal" und „RADIUS", um die Benutzer zu authentifizieren, die auf die serielle Schnittstelle zugreifen. Wenn die Authentifizierung auf „Local" (Lokal) eingestellt ist, authentifiziert das Gerät Benutzer anhand seiner eigenen Benutzerliste. Andernfalls fordert der Konsolenserver die Authentifizierung von externen Authentifizierungsservern (d.h. RADIUS) an. Die folgende Abbildung veranschaulicht das Verfahren bei der Benutzer-Authentifizierung über einen externen Server.

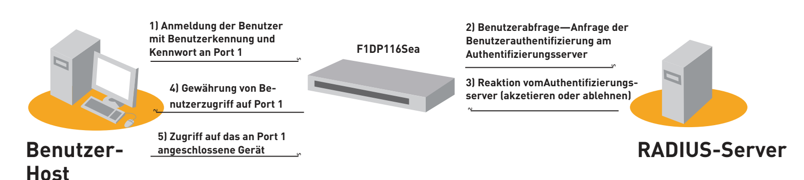
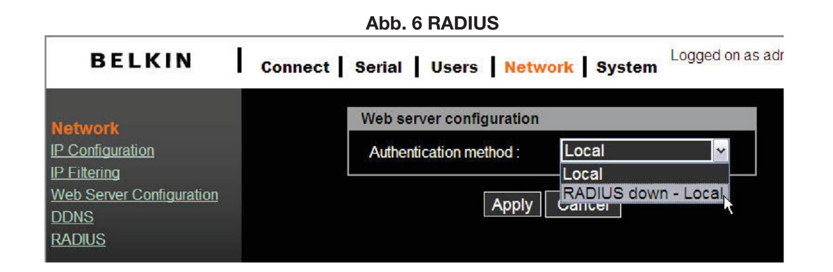
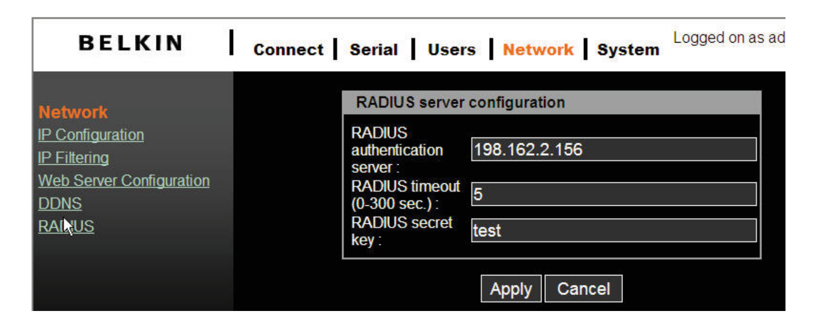


Abb. 6 RADIUS






RADIUS-Server-Konfiguration



> **Hinweis**:
> Um den RADIUS-Dienst in Kraft zu setzen, muss vorher ein RADIUS-Server installiert sein.

HTTPS/SSL

Der Konsolenserver unterstützt die Protokolle HTTP und HTTPS (HTTP über SSL) gleichzeitig. Sie können die Sicherheitsfunktion für jede Schnittstelle einzeln aktivieren oder deaktivieren.

HTTPS bietet eine sichere, verschlüsselte Web-Schnittstelle über SSL (Secure Sockets Layer).

Die folgenden Schritte müssen für das HTTPS-Protokoll verwendet werden:

1. Ändern Sie die URL von „http://xxx.xxx.xxx/" zu „https://xxx.xxx.xxx/".
2. Nach dem Aufbau der Verbindung wird im Browser ein Schloss-Symbol angezeigt.



Doppelklicken Sie auf das Schloss-Symbol, um ausführliche Zertifizierungsinformationen anzuzeigen.




Konfiguration

Klicken Sie unter der Menüüberschrift „Serial" (Seriell) auf „Configuration" (Konfiguration), um die Schnittstellen-Übersichtsliste anzuzeigen.



Serial port configuration

Individual port configuration

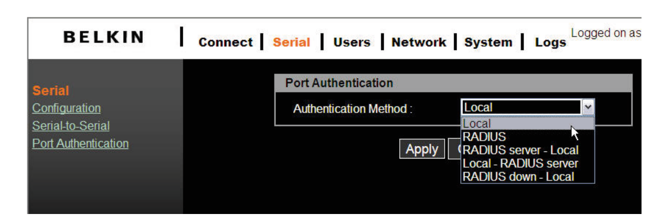
Port Number	Name	Mode	Dest/Assigned	Port	Proto	Serial-settings
1	Console Port 1	CS	-	4001	SSH	9600-N-8-1-No
2	Console Port 2	CS	-	4002	Telnet	9600-N-8-1-No
3	Console Port 3	CS	-	4003	Telnet	9600-N-8-1-No
4	Console Port 4	CS	-	4004	Telnet	9600-N-8-1-No
5	Console Port 5	CS	-	4005	Telnet	9600-N-8-1-No
6	Console Port 6	CS	-	4006	Telnet	9600-N-8-1-No
7	Console Port 7	CS	-	4007	Telnet	9600-N-8-1-No
8	Console Port 8	CS	-	4008	Telnet	9600-N-8-1-No
9	Console Port 9	CS	-	4009	Telnet	9600-N-8-1-No
10	Console Port 10	CS	-	4010	Telnet	9600-N-8-1-No
11	Console Port 11	CS	-	4011	SSH	9600-N-8-1-No
12	Console Port 12	CS	-	4012	Telnet	9600-N-8-1-No
13	Console Port 13	CS	-	4013	Telnet	9600-N-8-1-No
14	Console Port 14	CS	-	4014	Telnet	9600-N-8-1-No
15	Console Port 15	CS	-	4015	Telnet	9600-N-8-1-No
16	Console Port 16	CS	-	4016	Telnet	9600-N-8-1-No

Wenn „Serial Port" (Serielle Schnittstelle) deaktiviert ist, wird die Schnittstelle im Bereich „Serial port configuration" (Serielle Schnittstellenkonfiguration) dunkelgrau angezeigt. Aktivierte serielle Schnittstellen werden stets in weißer Schrift dargestellt.

Port-Authentifizierung

Durch die so genannte Authentifizierung wird eine Person, meist über Benutzername und Kennwort, identifiziert. Der Konsolenserver unterstützt verschiedene Authentifizierungsoptionen wie „Lokal" und „RADIUS", um die Benutzer zu authentifizieren, die auf die serielle Schnittstelle zugreifen. Weitere Angaben, siehe Seite 23.

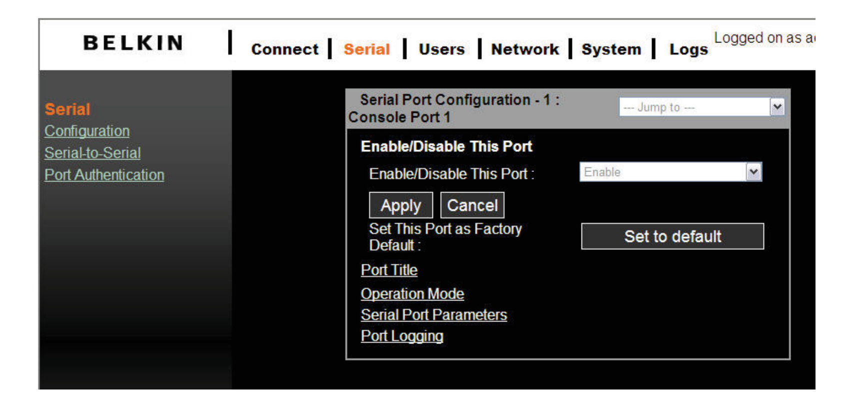
Wenn die Authentifizierung auf „Local" (Lokal) eingestellt ist, authentifiziert der Konsolenserver Benutzer anhand seiner eigenen Benutzerliste. Bei Konfiguration für RADIUS fordert der Konsolenserver die Authentifizierung von externen Authentifizierungsservern (d.h. RADIUS) an. Die folgende Abbildung veranschaulicht das Verfahren bei der Benutzer-Authentifizierung über einen externen Server.





Schnittstelle aktivieren/deaktivieren

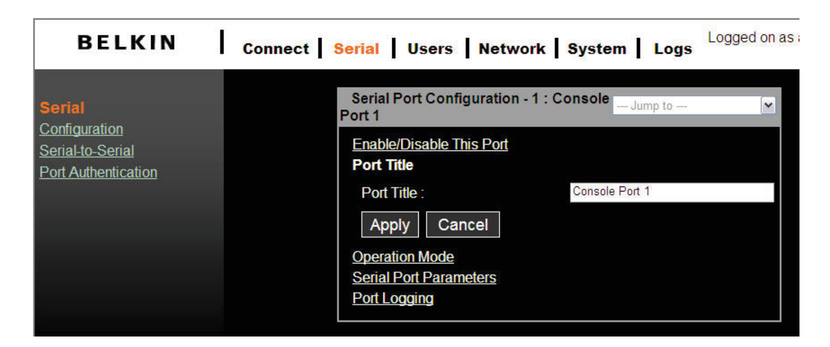
Jede serielle Schnittstelle kann einzeln aktiviert oder deaktiviert werden. Benutzer können nicht auf deaktivierte serielle Schnittstellen zugreifen. Sie können die serielle Schnittstelle jedoch mit der Schaltfläche „Set to default" (Auf Standard einstellen) auf die Standardeinstellungen zurücksetzen.






Schnittstellentitel

Benutzer können für jede Schnittstelle beschreibende Informationen zum angeschlossenen Gerät eingeben.



Mit der Verknüpfung „--Jump to--" (Wechseln zu) oben rechts können Sie eine andere Schnittstelle auswählen und konfigurieren.

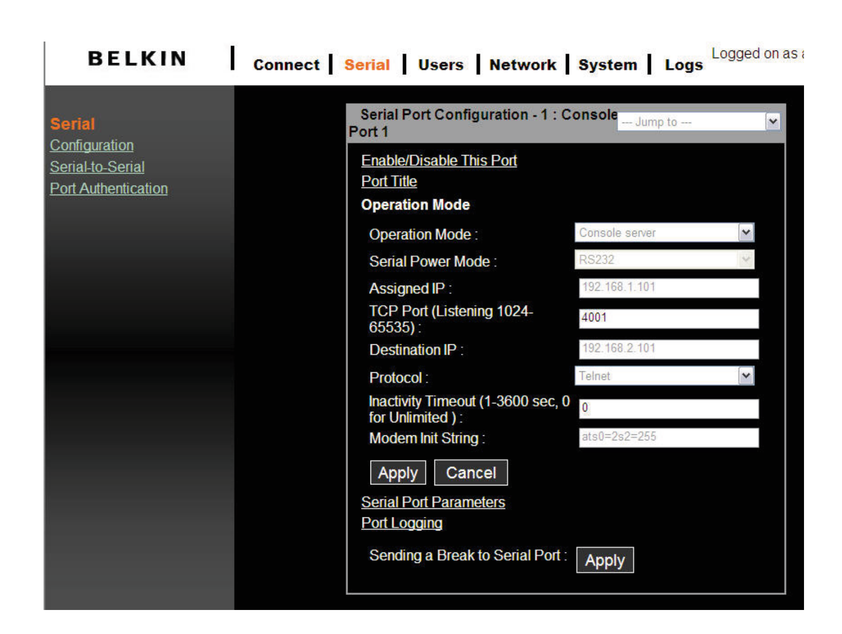



Betriebsmodi

Der Konsolenserver bietet vier verschiedene Betriebsmodi. Sie werden im folgenden beschrieben.

> **Hinweis**:
> - Der letzte Port (z. B. Port 16) kann im Seriell/Seriell-Betrieb auch als externer ESP (External ESP: Entry Serial Port). Weitere Informationen finden Sie im Abschnitt „Seriell/Seriell-Funktion"





Konsolenserver-Betrieb

Die Konfiguration einer seriellen Schnittstelle als Konsolenserver erzeugt eine TCP-Socket auf dem Gerät, das eine Telnet- oder SSH-Client-Verbindung abhört. Wenn Sie die Verbindung zu einer TCP-Socket herstellen, haben Sie Zugriff auf das Gerät, das an die serielle Schnittstelle angeschlossen ist, als wäre das Gerät direkt mit dem Netzwerk verbunden. Datenströme können in beiden Richtungen zwischen dem Gerät und dem Telnet-/SSH-Client-Programm ausgetauscht werden. RawTCP wird im Konsolenserver-Betrieb ebenfalls unterstützt.





Die folgenden Parameter können im Konsolenserver-Betrieb konfiguriert werden:

Listening TCP Port Number (Abhörende TCP-Schnittstellennummer)

Sie können über die IP-Adresse des Konsolenservers und der abhörenden TCP-Schnittstellennummer der seriellen Schnittstelle auf eine serielle Schnittstelle zugreifen.

Wenn als IP-Adresse des Konsolenservers und serielle Schnittstelle 192.168.123.100 zugewiesen ist und die abhörende TCP-Schnittstellennummer 4001 lautet, kann der Benutzer die Schnittstellenverbindung folgendermaßen aufbauen: telnet 192.168.123.100 4001

Protokoll

Wählen Sie „Telnet", „SSH" oder „Raw TCP" als Protokoll aus. Wenn die Benutzer ein Telnet-Client-Programm einsetzen, wählen Sie „Telnet". Wenn die Benutzer ein SSH-Client-Programm einsetzen, wählen Sie „SSH". Wenn Sie „Raw TCP" wählen, ist zwischen dem Konsolenserver und dem entfernten Host eine direkte TCP-Socket-Kommunikation möglich.

Inactivity Time-Out (Zeitlimit)





Aktivieren Sie diese Funktion, wenn ein Client nach längerer Inaktivität an einer seriellen Schnittstelle die TCP-Verbindung freigeben soll. Wenn „Inactivity timeout" (Inaktivitätszeitlimit) ist und im gewählten Zeitlimit keine Datenaktivität zwischen dem Konsolenserver und dem Telnet/SSH-Client festzustellen ist (d. h. keine Datenaktivität über die serielle Schnittstelle), wird die bestehende TCP-Sitzung automatisch geschlossen. Wenn Sie die Verbindung unbefristet aufrecht erhalten möchten, stellen Sie als Zeitlimit „0" ein.

TCP Keep-Alive (No Configuration Required) (TCP-Nichtbedienungszeit / TCP-Aufrechterhaltung)

Um eine TCP-Verbindungsblockade zu verhindern, überprüft der Konsolenserver weiterhin den Verbindungsstatus zwischen dem Telnet/SSH-Client und dem Konsolenserver durch die regelmäßige Übertragung von Aufrechterhaltungspaketen. Wenn der Telnet/SSH-Client nicht auf die Pakete antwortet, nimmt das System an, dass die Verbindung nicht mehr verfügbar ist. Der Konsolenserver schließt dann die bestehende Telnet/SSH-Verbindung unabhängig von der Inaktivitätseinstellung. Dadurch wird verhindert, dass die TCP-Verbindung blockiert, wenn eine Anwendung nicht sauber geschlossen oder eine Netzwerkverbindung unterbrochen wird.

Terminalserver-Betrieb

Im Terminalserver-Betrieb wartet die serielle Schnittstelle des Konsolenservers auf Daten aus dem mit ihr verbundenen Gerät. Werden Daten erkannt, startet der Konsolenserver eine TCP-Sitzung als Telnet- oder SSH-Client eines vordefinierten Servers. Der Server muss von Benutzern definiert werden, bevor die Schnittstelle für einen Telnet- oder SSH-Client konfiguriert werden kann. In diesem Betriebsmodus können Server im Netzwerk von einem seriellen Terminal aus angesprochen werden. RawTCP wird im Terminalserver-Betrieb ebenfalls unterstützt.

```
Terminal server mode (ssh), press any key ...
login:root
passwd:
login as:jeffrey
The authenticity of host '192.168.123.164 (192.168.123.164)' can't be establishe
d.
  RSA key fingerprint is 1c:92:81:af:9f:a7:b5:1f:7c:ab:dc:d9:b7:46:f1:ef.
                                                                         Are you
 sure you want to continue connecting (yes/no)? yes
jeffrey@192.168.123.164's password:
[jeffrey@Jeffrey_Linux jeffrey]$ ls
lincvs-1.3.1-2-RedHat-9.0-i386-bin.rpm  proj                        tmp
lincvs-1.4.3                            qt-x11-free-3.3.3           util
lincvs-1.4.3-0-generic-src.tar          qt-x11-free-3.3.3.tar.bz2
[jeffrey@Jeffrey_Linux jeffrey]$          ← Ctrl-Z / Ctrl-X / Ctrl-C
Terminal server mode (ssh), press any key ...
```


Zur Beendigung einer Telnet/SSH/RawTCP-Sitzung im Terminalserver-Betrieb können Sie diese drei STRG-Tastenfolgen nutzen: Strg-Z / Strg-X / Strg-C).




DFÜ-Modem-Betrieb

In diesem Betriebmodus nimmt der Konsolenserver an, dass ein externes Modem an der seriellen Schnittstelle angeschlossen ist und wartet auf eine eingehende Fernwahlverbindung. Wenn sich ein Benutzer über eine Terminal-Anwendung einwählt, nimmt der Konsolenserver die Verbindung an und zeigt die Eingabeaufforderung oder das Menü für den angemeldeten Benutzer an.

Seriell/Seriell-Betrieb

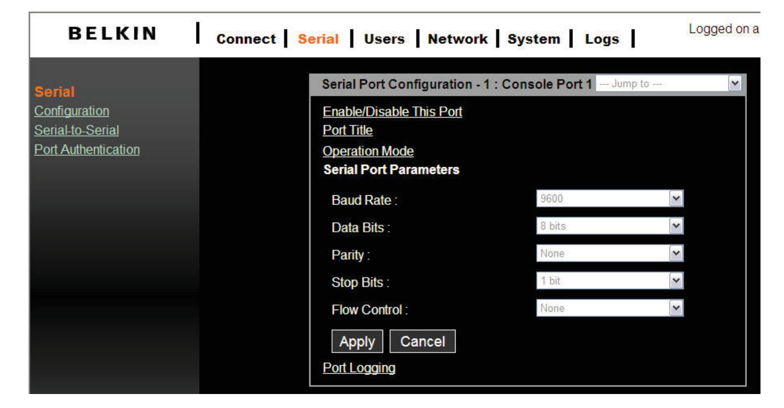
Einzelheiten zu diesem Betriebmodus finden Sie auf Seite 34 im Abschnitt „Seriell/Seriell-Funktion".

Serielle Schnittstellenparameter

Beim Anschluss des seriellen Geräts an die serielle Schnittstelle des Konsolenservers müssen die Parameter der seriellen Serverschnittstelle den Anforderungen des angeschlossenen seriellen Geräts genau entsprechen.

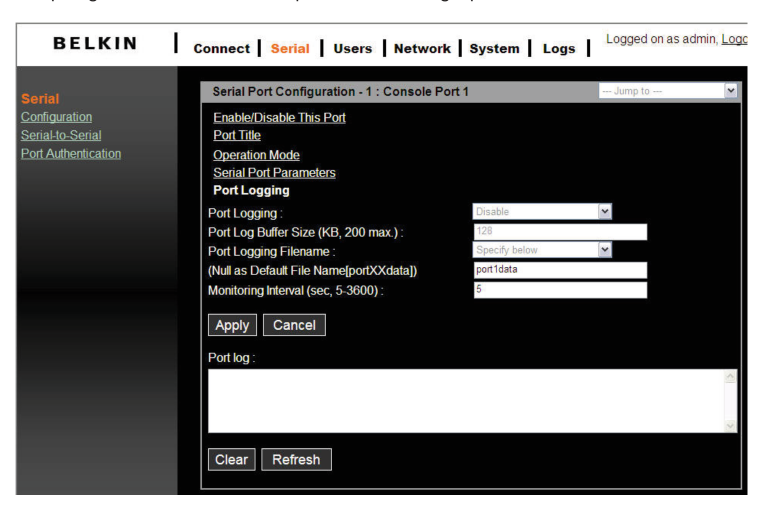




Schnittstellenprotokollierung

Im Konsolenserver-Betrieb werden die aus der verfolgenden seriellen Schnittstelle empfangenen Daten im Gerätespeicher zwischengespeichert.



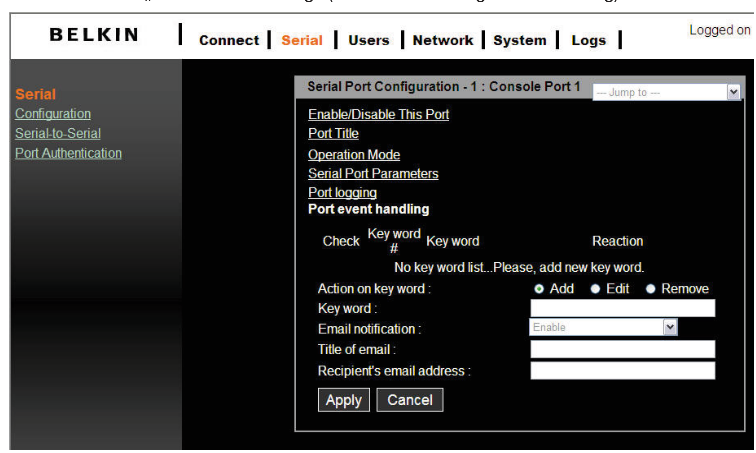
Die Schnittstellenprotokollierung ist nur im Konsolenserver-Betrieb der seriellen Schnittstelle als Option verfügbar.

Wenn die Option „Port logging" (Schnittstellenprotokollierung) aktiviert ist, kann der Benutzer den Konsolenserver in den Protokolldaten nach einem festgelegten Schlüsselwort suchen lassen und dem Administrator anhand der Einstellungen für die Schnittstellen-Ereignisverarbeitung eine E-Mail zukommen lassen. Jede Reaktion kann für jedes Schlüsselwort einzeln konfiguriert werden. Die Reaktion kann über eine E-Mail erfolgen.





Klicken Sie auf „Port event handling" (Schnittstellenereignisverarbeitung).



Der Pufferspeicher zur Protokollierung von Daten beträgt 192 KB pro Anschluss. Übersteigen die Protokolldaten den verfügbaren Speicher, werden alte durch neue Daten überschrieben.




Unterbrechungsfunktion

Im Konsolenserver-Betrieb kann der Konsolenserver dem angeschlossenen seriellen Gerät ein Unterbrechungssignal senden. Mit einem Unterbrechungssignal wird zuweilen eine Kommunikationsleitung zurückgesetzt oder der Betriebsmodus der Kommunikationshardware, z. B. eines Modems, geändert. Bestimmte Zielgeräte wie der Sun™ Solaris™ Server benötigen ein Nullzeichen (Unterbrechungssignal), um eine „OK"-Eingabeaufforderung zu erzeugen. Die Übermittlung eines Unterbrechungssignals über die serielle Schnittstelle hat die gleiche Wirkung wie ein „STOP-A" auf einer SUN-Tastatur. Um ein Unterbrechungssignal an ein serielles Gerät zu übermitteln, setzen Sie es in den Konsolenserver-Betrieb und verwenden Sie „Telnet" oder „RawTCP" als Protokoll. Klicken Sie auf die Schaltfläche „Apply" (Übernehmen), um ein Unterbrechungssignal an die bezeichnete serielle Schnittstelle und dann an den angeschlossenen Computer oder Server zu übertragen.

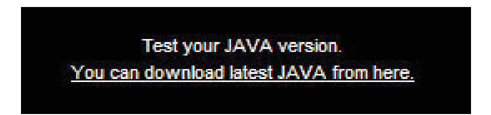
Verbindung

Der Konsolenserver bietet webgestützten Zugriff auf ein serielles Zielgerät, ohne dass ein separates Telnet-Client-Programm benötigt wird. Der Zugriff wird über ein Java-Applet ermöglicht.

Über ein Java-Applet erhält die textbasierte Benutzeroberfläche Zugriff auf die serielle Schnittstelle. Das Java-Applet unterstützt im Konsolenserver-Betrieb nur Telnet. Der Benutzer kann nicht über das Web auf die serielle Schnittstelle zugreifen, wenn als Host-Betrieb der Schnittstelle eine RawTCT-Verbindung konfiguriert ist. Für den Zugriff auf die Schnittstelle wird der Benutzer zur Eingabe von Benutzerkennung und Kennwort aufgefordert. Nach der Authentifizierung kann der Benutzer auf die serielle Schnittstelle zugreifen.



Testen Sie die Java-Kompatibilität mit dem Hyperlink unten auf der Verbindungsseite. Mit dem Link unten können Sie die aktuelle Java-Version herunterladen.



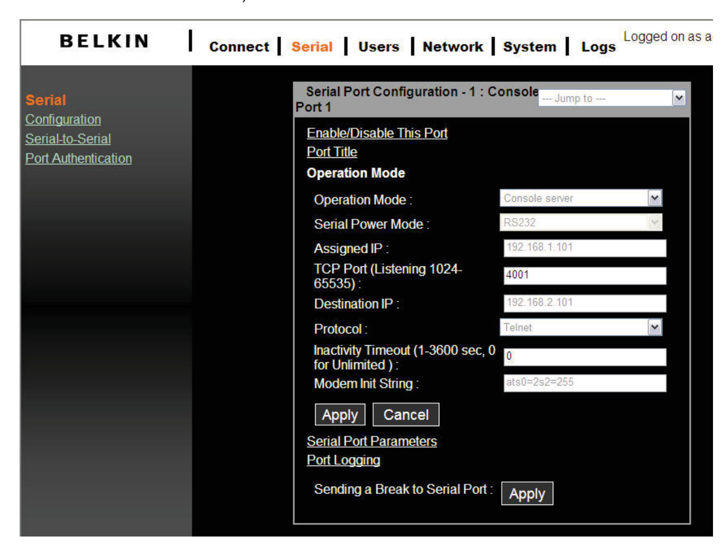
Aktivieren Sie die Java-Option Ihres Browsers (soweit noch nicht geschehen) und überprüfen Sie die Versionsnummer Ihrer Java-Laufzeitumgebung (auch als „JRE-Version" bezeichnet). Wenn Sie auch den abgesicherten HTTP-Dienst (HTTPS) nutzen möchten, benötigen Sie mindestens Version 1.6.0.

Hinweis:

- Um diese Funktion auszuführen, ist die Installation von JRE, Version 6.0 oder höher erforderlich. Sie finden die Java-Software auf der Website http://www.java.com/en/download/.

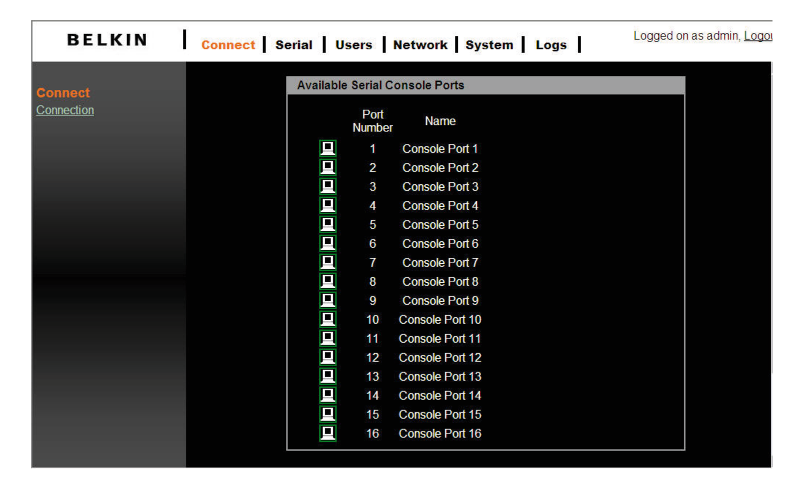
Telnet Java-Applet

1. Wählen Sie unter „Serial > Configuration > Operation mode" (Seriell > Konfiguration > Betriebsmodus) das Telnet-Protokoll aus.

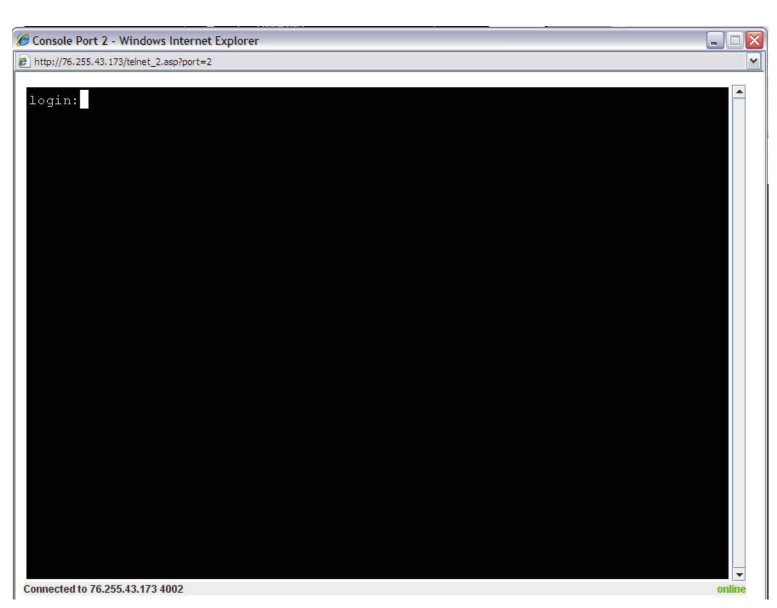


Wählen Sie im Hauptmenü die Option „Connect" (Verbinden) und klicken Sie auf das Terminalsymbol links. Die Terminal-Emulation wird in einem neuen Fenster geöffnet und fordert Sie zur Anmeldung auf. Wenn nur ein leeres Fenster zu sehen ist, überprüfen Sie, ob Ihre Java-Version mit Ihrem System kompatibel ist.



2. Geben Sie zur Anmeldung Benutzername und Kennwort ein, damit die Emulation wie ein laufendes Telnet-Client-Programm (z.B., Telnet DOS-Programm, PuTTY) verwendet werden kann.



Hinweis: Der Name der aktiven seriellen Schnittstelle wird in der Fensterleiste angezeigt. Zudem wird unten rechts im Fenster eine Verbindungsstatusanzeige eingeblendet.





Seriell/Seriell-Funktion

Anhand der Seriell/Seriell-Funktion können Sie mit einem einfachen Terminal (Display mit Tastatur) Geräte ansteuern und kontrollieren, die an den Schnittstellen 1 bis 15 mit dem Konsolenserver verbunden sind. Sie können auch einen externen Terminalkonverter wie den Belkin F1D084Eea verwenden, um den Konsolenserver mit einem KVM-Switch verbinden und dadurch die Kontrolle zu zentralisieren.

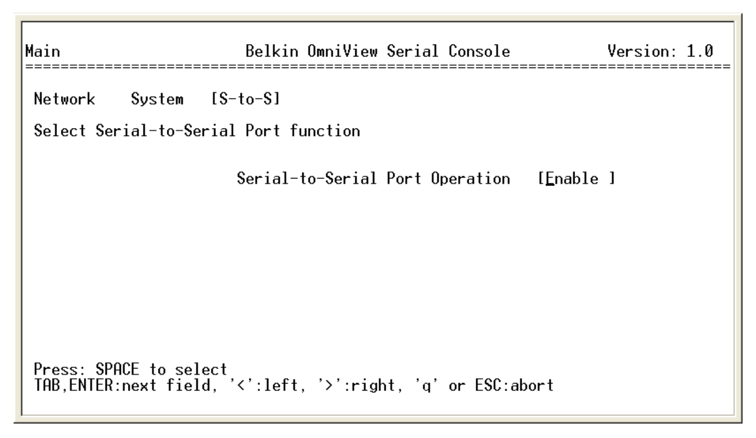
Installation

Schließen Sie das Terminal an Schnittstelle 16 des Konsolenservers an. Dadurch können Sie ausschließlich über die Schnittstellen 1 bis 15 auf ein serielles Gerät zugreifen.

Seriell/Seriell aktivieren und konfigurieren

So konfigurieren Sie die Seriell/Seriell-Funktion:

1. Wechseln Sie in den VT-100-Konsolenbetrieb (siehe Abschnitt „Zuweisen der IP-Adresse über die Konsolenschnittstelle VT-100 (Konsole, Telnet, SSH)", um das Fenster unten zu öffnen.
2. Wählen Sie in Menüebene 2 die Option [S-to-S] „Serial-to-Serial port Operation" (Seriell/Seriell-Schnittstellenbetrieb) und drücken Sie die Leertaste, um „ENABLE" (Aktivieren) zu wählen. Bestätigen Sie die Änderung, um das System automatisch neu zu starten.



3. Trennen Sie jetzt die Verbindung an der lokalen Konsole und starten Sie eine neue Terminalsitzung durch Aufbau einer Verbindung mit Schnittstelle 16.
4. Nach dem Neustart (ca. eine Minute) wird das auf der folgenden Seite gezeigte Fenster geöffnet. Konfigurieren Sie die einzelnen Einstellungen. Geben Sie den Wert für „Inactivity timeout" (Inaktivitätszeitlimit) ein und drücken Sie die Leertaste, um die Einstellung für die anderen Optionen festzulegen.

Hinweis:

- Wenn auf dem Bildschirm das folgende Fenster für die Seriell/Seriell-Konfiguration angezeigt werden soll, muss die Funktion Seriell/Seriell aktiviert sein. Die Standard-Baudrate ist auf 9600 8N1 festgelegt (nicht rekonfigurierbar), damit eine optimale Kompatibilität mit Terminal-Bildschirmen von Drittherstellern gewährleistet werden kann.

```
                         Belkin OmniView Serial Console          Version: 1.0
================================================================================
[S-to-S]

 Serial-to-Serial Configuration


                        Connect to Port#     [_2]
                        Inactivity Timeout   [0         ]
                        Baud Rate            [9600  ]
                        Data Bits            [8 bits]
                        Parity               [None]
                        Stop Bits            [1 bit ]
                        Flow Control         [None    ]



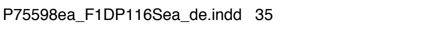

 Press: SPACE to select
 TAB,ENTER:next field, '<':left, '>':right, 'q' or ESC:abort
```

5. Wählen Sie die gewünschte Schnittstellennummer für die Verbindung. Daraufhin wird das folgende Fenster geöffnet.

```
Serial-to-Serial mode , press any key ...
login:admin
password:
```

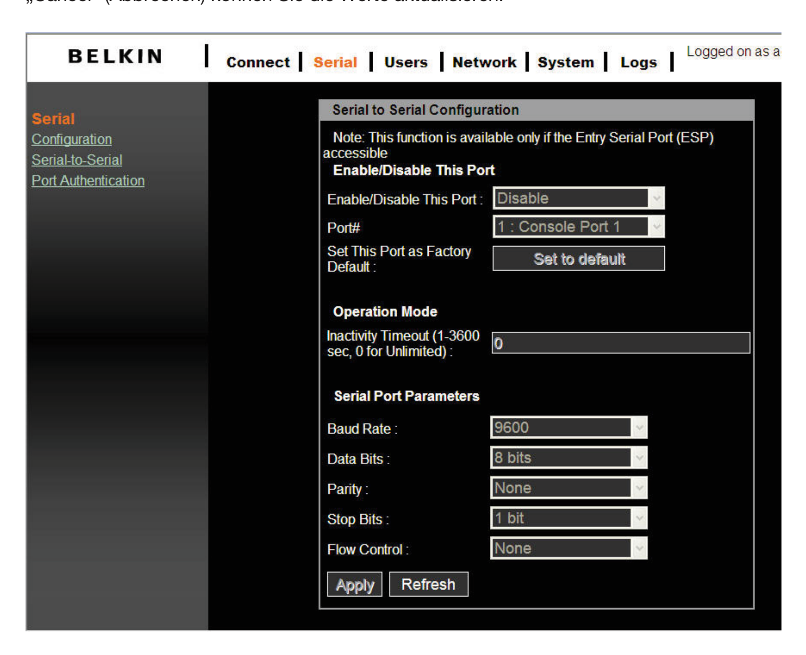
6. Geben Sie den Benutzernamen und das Kennwort ein. Die Datenkanalverbindung zwischen Schnittstelle 16 und der gewählten seriellen Schnittstelle wird aufgebaut, so dass der Administrator das serielle Gerät oder den Server kontrollieren kann.
7. Drücken Sie die STRG- und die C-Taste, um die Seriell/Seriell-Funktion zu beenden und in das Konsolenhauptfenster zurückzukehren.





Die Webseite zeigt auch schreibgeschützte Einstellungen der Seriell/Seriell-Funktion an. Die Einstellungsänderungen über die VT-100-Konsole werden automatisch übernommen. Mit „Cancel" (Abbrechen) können Sie die Werte aktualisieren.

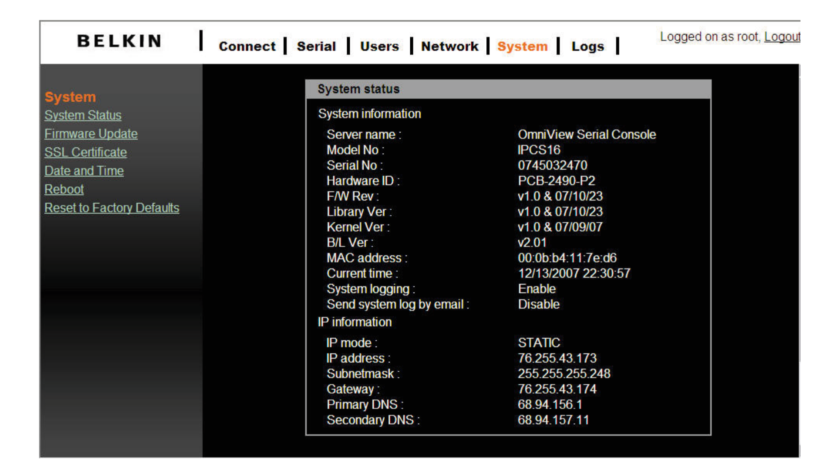







Systemstatus

Auf der Seite „System Status" (Systemstatus) werden die aktuellen Systeminformationen wie Name, Seriennummer, Firmware-Versionen, MAC-Adresse, aktuelle Uhrzeit und Netzwerkeinstellungen angezeigt. Auf diese Seite können keine Daten geändert werden. Die Seite wird automatisch alle 10 Sekunden aktualisiert.





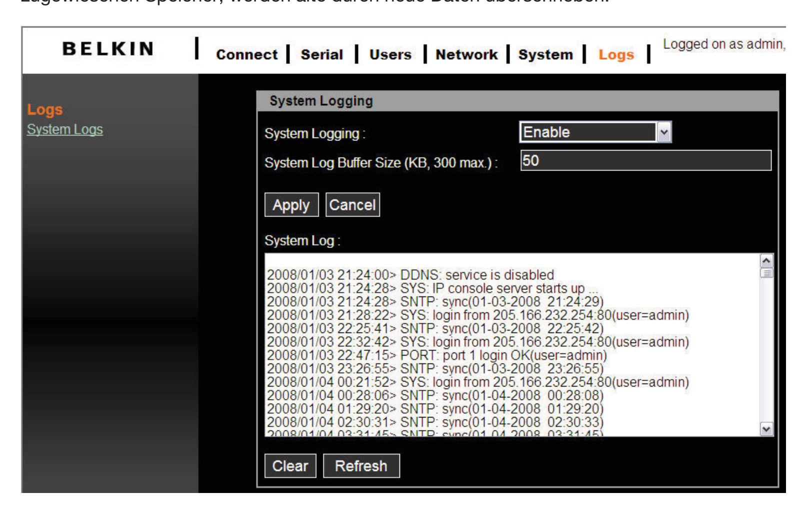






Systemprotokollierung

Sie können die Systemprotokollierung aktivieren bzw. deaktivieren und die Protokollpuffergröße einstellen. Der Standardwert für den Protokollpufferspeicher beträgt 50 KB und kann auf bis zu 300 KB erhöht werden. Übersteigen die Protokolldaten den zugewiesenen Speicher, werden alte durch neue Daten überschrieben.






Die folgenden Systemereignisse werden zyklisch im flüchtigen Speicher protokolliert:

i) SYS (Systemstart, Ausfallzeit, Benutzerkonto-Authentifizierung)

ii) SNTP (Netzwerkzeit-Synchronisierung)

iii) LOG (Systemereignisprotokoll löschen)

iv) PORT (Authentifizierung für Zugriff auf serielle Schnittstelle)

v) DDNS (Ereignis der dynamischen IP-Adresse registrieren)







Benutzerverwaltung

Beim Systemstart wird der Benutzer zur Kennworteingabe aufgefordert, um auf das System zuzugreifen. Der Administrator kann einen Benutzer über die Webseiten einfach und problemlos hinzufügen oder entfernen.

Für die Zugriffsrechte werden zwei Stufen angeboten:

Benutzername	Standard-Kennwort	Zugriffsrechte
admin	admin	Admin.-Zugriff
(Benutzername)	(Benutzername)	Nur Zugriff auf „Serial Port" (Serielle Schnittstelle) und „System Status" (Systemstatus)

Wenn der Benutzer nicht zum Zugriff auf die Webseite berechtigt ist, erscheint eine Seite mit einer Verweigerungsmeldung.





Benutzer hinzufügen

So fügen Sie einen Benutzer hinzu:

- Überprüfen Sie die Benutzer im Fenster „User administration" (Benutzerverwaltung).
- Klicken Sie auf die Schaltfläche „Add" (Hinzufügen).
- Geben Sie den neuen Benutzernamen und das neue Kennwort ein.

Regeln für Benutzername und Kennwort

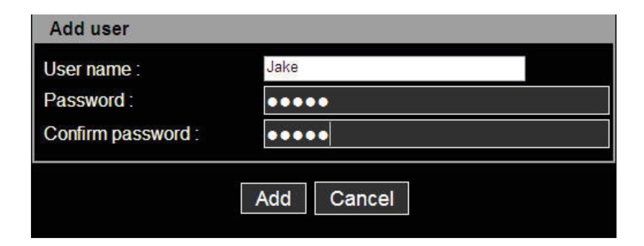
- Das erste Zeichen des Benutzernamens muss ein Buchstabe sein.
- Das Kennwort muss aus mindestens drei Zeichen bestehen.
- Der Benutzername bzw. das Kennwort darf nicht mehr als 32 Zeichen enthalten.
- Nur „admin"-Benutzer können auf „Network" (Netzwerk) und „System administration" (Systemverwaltung) zugreifen.







Die nachstehende Abbildung zeigt das Fenster „Add User" (Benutzer hinzufügen).



Der neue Benutzer wird in der Liste „User Name" (Benutzername) angezeigt.






Benutzer entfernen

So entfernen Sie einen Benutzer:

- Überprüfen Sie die Benutzer im Fenster „User administration" (Benutzerverwaltung).
- Klicken Sie auf die Schaltfläche „Remove" (Entfernen).





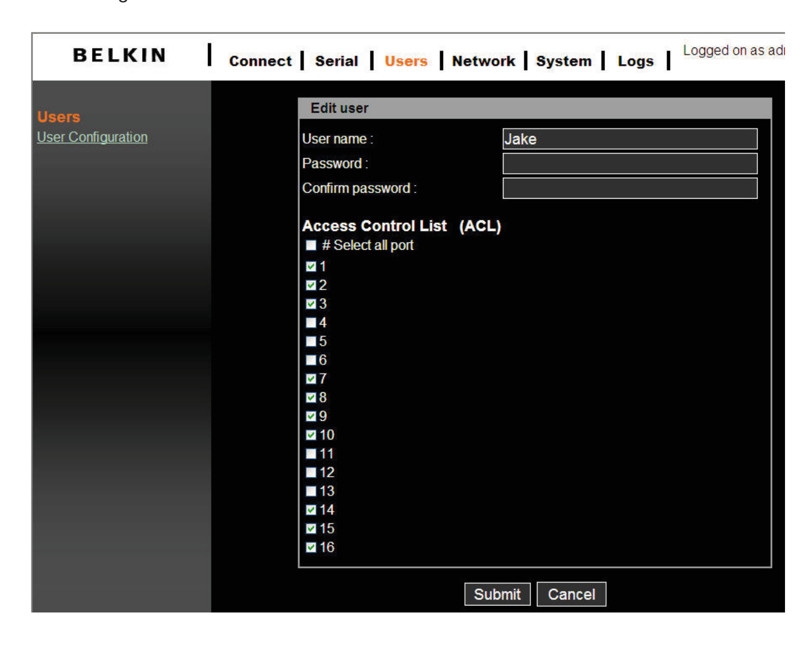
Die Zugriffskontrollliste (ACL) bearbeiten

Der Konsolenserver bietet Sicherheit über Zugriffskontrolllisten, in denen Sie den Benutzerzugang differenziert nach einzelnen Anschlüssen bestimmen können.

So bearbeiten Sie die Zugriffskontrollliste:

- Überprüfen Sie die Benutzer im Fenster „User administration" (Benutzerverwaltung).
- Klicken Sie auf die Schaltfläche „Edit" (Bearbeiten).
- Geben Sie den Benutzernamen und das Kennwort ein.
- Wählen Sie die Schnittstelle aus, auf die Sie zugreifen möchten.
- Klicken Sie auf die Schaltfläche „Submit" (Absenden).

Nach dem Festlegen der Zugriffskontrollliste für das Benutzerkonto können Benutzer ausschließlich auf die autorisierten seriellen Schnittstellen zugreifen oder deren Einstellungen verändern. Die Benutzer können nicht autorisierte serielle Schnittstellen weder anzeigen noch konfigurieren.









Kennwort ändern

Um die Parameter des Benutzerkontos zu ändern, öffnen Sie das Fenster „Edit user" (Benutzer bearbeiten), in dem Sie den Benutzernamen im Fenster „User Configuration" (Benutzerkonfiguration) wählen und dann die Parameter des Kontos bearbeiten, zum Beispiel durch das Hinzufügen eines Benutzers.

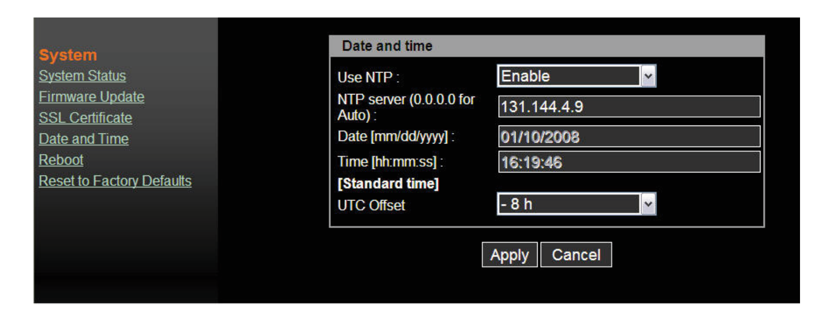
Datum und Zeit (NTP)

Der Konsolenserver behält die aktuellen Datums- und Uhrzeitinformationen bei. Die Uhr- und Kalendereinstellungen werden durch eine interne Batterie gesichert. Der Benutzer kann das aktuelle Datum und die Uhrzeit einstellen.

Zum Einstellen von Datum und Uhrzeit stehen zwei Möglichkeiten zur Verfügung. Der NTP-Server kann die Datums- und Uhrzeiteinstellungen steuern. Wenn die NTP-Funktion aktiviert ist, erhält der Konsolenserver die Datums- und Uhrzeitinformationen bei jedem Neustart vom NTP-Server und gleicht sie danach stündlich mit dem NTP-Server ab. Wenn der NTP-Server auf die Adresse 0.0.0.0 gesetzt ist, verwendet der Konsolenserver automatisch die Standard-NTP-Server. In diesem Fall sollte er vom Netz mit dem Internet verbunden werden. Als zweite Möglichkeit können Datum und Uhrzeit manuell ohne NTP-Server eingestellt werden. In diesem Fall werden die Datums- und Uhrzeitinformationen durch die interne Batterie aufrecht erhalten.




In der Meteorologie beziehen sich alle Zeitangaben standardmäßig auf die Westeuropäische Zeit (GMT). Sie wird auch als Koordinierte Weltzeit (Kürzel: UTC) bezeichnet. Sie können die Zeitzone und die Zeitdifferenz zur Koordinierten Weltzeit an den Benutzerstandort anpassen, um Systemdatum und -Uhrzeit genau festzulegen. Die Zeitdifferenz „x" (Feld „Time offset") kann als positive oder negative ganze Zahl festgelegt werden. Unter http://time_zone.tripod.com/ finden Sie die Zeitdifferenzen der einzelnen Zeitzonen zur Koordinierten Weltzeit.





Hinweis:

- Der Konsolenserver ist mit einer Echtzeituhr-Funktion (RTC: Real-Time Clock) ausgestattet und wird über eine Lithium-Knopfzelle (CR2032, 3 V) mit Strom versorgt. So werden Datum und Zeit auch bei Stromausfall korrekt angezeigt.
- Wenn die Zeit- und Datumsdaten wiederholt verloren gehen, sollten Sie die Knopfzelle ersetzen.
- Ersetzen Sie die 3-Volt CR203-Knopfzelle nur durch denselben oder einen vergleichbaren vom Hersteller empfohlenen Typen.   Eine neue Batterie/Knopfzelle kann explodieren, wenn Sie nicht ordnungsgemäß eingesetzt wird. Entsorgen Sie leere Batterien entsprechend den Anweisungen des Herstellers.

Firmware-Upgrade

Firmware kann auf einfache Weise über eine Webseite aktualisiert werden. In diesem Kapitel wird Aktualisierungsverfahren beschrieben.

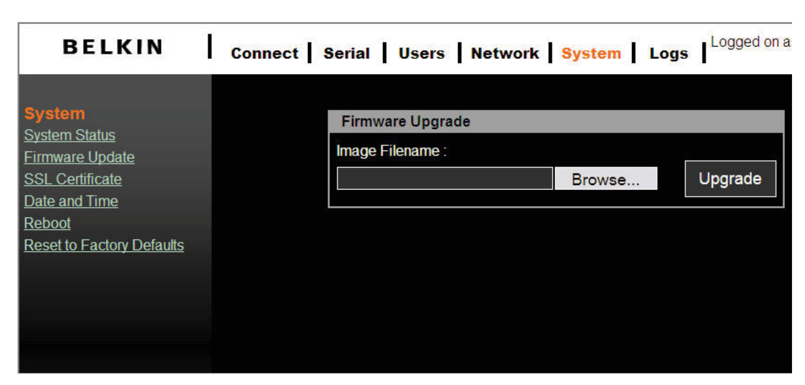
Die neueste Firmwareversion erhalten Sie unter www.belkin.com/support.

Upgrade über die Web-Oberfläche

Nähere Informationen finden Sie auf der Webseite „System > Firmware Upgrade" (System > Firmware-Upgrade).







Klicken Sie auf „Browse" (Durchsuchen), um die Firmware-Datei über den Explorer zu suchen. Navigieren Sie durch den PC und wählen Sie die Firmware-Datei aus. Klicken Sie zur Bestätigung auf „OK"

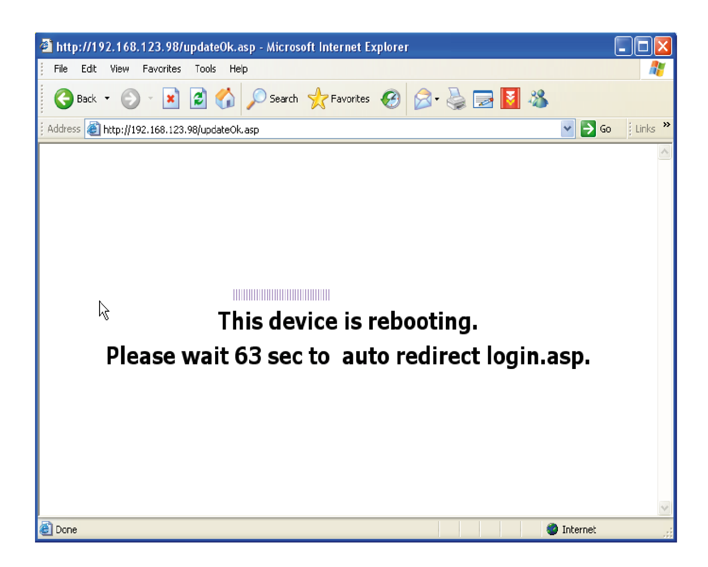
Klicken Sie nach dem Auswählen der Firmware-Datei auf „Upgrade", um die Firmware-Aktualisierung einzuleiten. Auf der Web-Oberfläche wird der Verlauf der Dateiübertragung in einer Statusanzeige angezeigt. Gleichzeitig blinkt die Anschluss-LED auf der Gerätevorderseite auf, um auf das Upgrade-Verfahren hinzuweisen.





Achtung! KEINESFALLS während des Upgrades den Strom abschalten oder das Ethernet-Kabel lösen! Dadurch könnte das Upgrade fehlschlagen und das Abbild im Speicher zerstört werden.

Der Konsolenserver führt nach dem Upgrade automatisch einen Neustart durch, um die neue Firmware zu aktivieren. Nach dem Ablauf der Zählung führt Sie der Browser zur Anmeldeseite. Auf der Seite „System Status" (Systemstatus) können Sie die Firmware-Version prüfen und das Upgrade bestätigen.

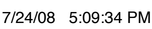




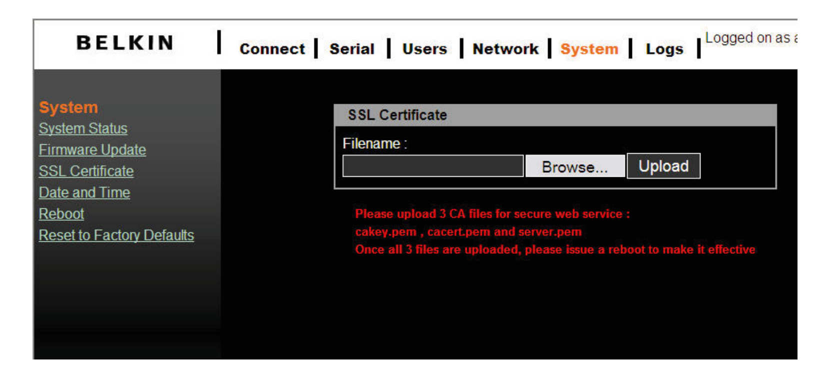
SSL-Zertifikat

Ein SSL-Zertifikat ist ein digitaler Ausweis für eine bestimmte Person, einen Betrieb, einen Server oder eine andere Einheit, die im Zertifikat ausgewiesen wird. Der Konsolenserver unterstützt für Konfigurationsänderungen über die Webseite sicheres HTTP (auch als HTTPS bezeichnet). Das serverseitige SSL-Zertifikat weist den Konsolenserver aus, so dass Sie sich auf das Zertifikat verlassen und Konfigurationsänderungen vertrauensvoll vornehmen können.

Der Konsolenserver kann benutzerdefinierte Zertifikatdateien auf den Webserver hochladen. Das Zertifikatdateipaket besteht aus drei Dateien (cacert.pem, cakey.pem, and server.pem). Alle drei Zertifikatdateien müssen für eine vollständige Aktualisierung des Zertifikats hochgeladen werden. Das Verfahren beim Hochladen entspricht dem Firmware-Upgrade.



Nach dem Hochladen aller Zertifikatdateien müssen die Benutzer einen manuellen Neustart einleiten, damit das neue Zertifikat wirksam wird.



Suchen Sie nach den vorbereiteten CA-Dateien (die Vorbereitung der drei CA-Dateien unter einem einheitlichen Dateinamen wird in Anlage E beschrieben) und laden Sie sie auf den Konsolenserver hoch. Überprüfen Sie nochmals jede Datei, bevor Sie sie hochladen. Ein falsches CA-Dateipaket kann zur Deaktivierung der HTTPS-Funktion führen.

Hinweis:

- Wenn CA-Dateien beschädigt sind, können Benutzer diese über „System > Reset to Factory Defaults” (System > Werkseinstellungen wiederherstellen) auf die Werkseinstellung zurücksetzen. Die alten CA-Dateien werden wiederhergestellt.
- Da der Name des Pfads der CA-Datei auf 256 Zeichen beschränkt ist, empfehlen wir Ihnen, für eine einfache Verwaltung alle Dateien unter „C:\upgrade” zu speichern.
- In Anhang E finden Sie Informationen zur Erstellung von CA-Dateien.

HTTPS-Zertifikat

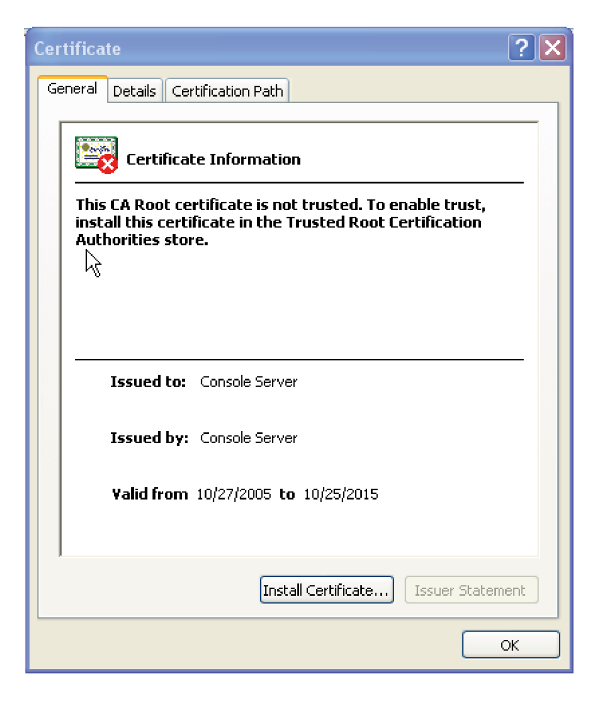
Ein sicherer Konsolenserver-Webdienst wird durch die https-Verbindung des Browsers (Dienstschnittstelle 443) ausgelöst. Der Browser weist Sie in einer Sicherheitsmeldung auf das Zertifikat hin. Sie müssen das Zertifikat akzeptieren, um den sicheren Webdienst zu starten. Benutzer können mit „View Certificate" (Zertifikat anzeigen) nachprüfen, ob der verbundene Webserver vertrauenswürdig ist.







Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate



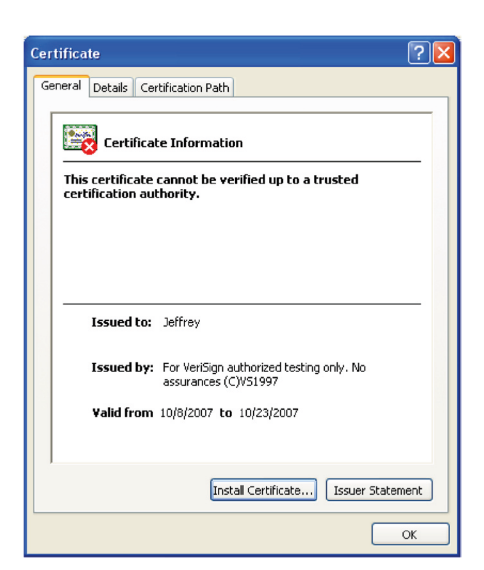
Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: Console Server
Issued by: Console Server
Valid from 10/27/2005 to 10/25/2015
Install Certificate...
Issuer Statement
OK




Eine andere Möglichkeit zur Unterscheidung sicherer von unsicheren Web-Verbindungen ist das Schloss-Symbol im Browser (im Internet Explorer unten rechts). Durch einen Doppelklick auf das Symbol können Sie detaillierte Informationen zum serverseitigen Zertifikat abrufen.

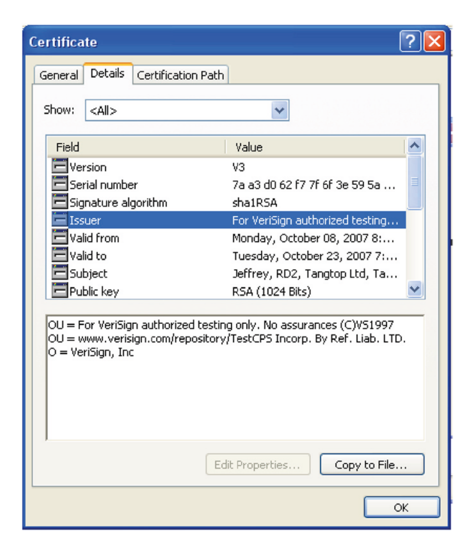
Nachdem Sie ein öffentlich signiertes CA-Dateipaket generiert haben, laden Sie es auf der Seite „SSL Certificate" (SSL-Zertifikat) hoch. Damit es wirksam wird, muss das System neu gestartet werden.

Das folgende Beispiel zeigt ein öffentlich signiertes Zertifikat mit Informationen, die bei der Zertifizierungsstelle (VeriSign) registriert sind.

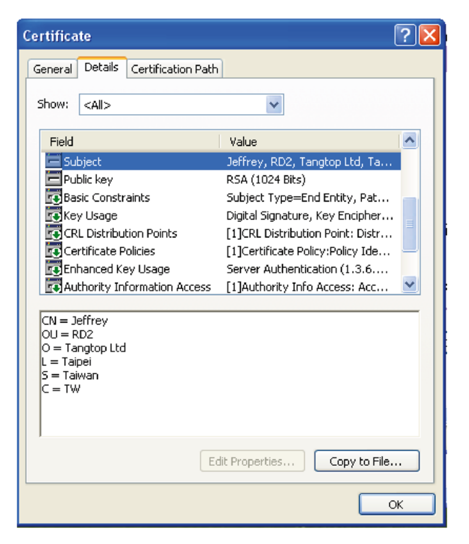







Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
7a a3 d0 62 f7 7f 6f 3e 59 5a ...
Signature algorithm
sha1RSA
Issuer
For VeriSign authorized testing...
Valid from
Monday, October 08, 2007 8:...
Valid to
Tuesday, October 23, 2007 7:...
Subject
Jeffrey, RD2, Tangtop Ltd, Ta...
Public key
RSA (1024 Bits)
OU = For VeriSign authorized testing only. No assurances (C)VS1997
OU = www.verisign.com/repository/TestCPS Incorp. By Ref. Liab. LTD.
O = VeriSign, Inc
Edit Properties...
Copy to File...
OK





Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
Jeffrey, RD2, Tangtop Ltd, Ta...
Public key
RSA (1024 Bits)
Basic Constraints
Subject Type=End Entity, Pat...
Key Usage
Digital Signature, Key Encipher...
CRL Distribution Points
[1]CRL Distribution Point: Distr...
Certificate Policies
[1]Certificate Policy:Policy Ide...
Enhanced Key Usage
Server Authentication (1.3.6....
Authority Information Access
[1]Authority Info Access: Acc...
CN = Jeffrey
OU = RD2
O = Tangtop Ltd
L = Taipei
S = Taiwan
C = TW
Edit Properties...
Copy to File...
OK





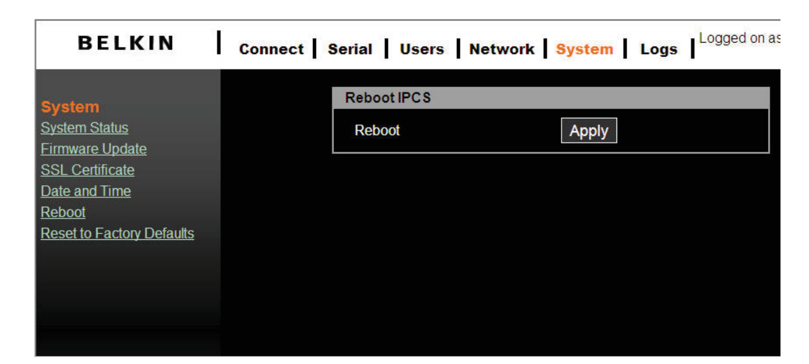
Werkseinstellungen wiederherstellen

Um die Werkseinstellungen wiederherzustellen, klicken Sie auf „Apply" (Übernehmen).



Neustart

Sie können über das Netzwerk auf dem Konsolenserver einen Software-Neustart einleiten. Der Neustart ist zwingend, nachdem das CA-Zertifikat vollständig hochgeladen worden ist.









Standardeinstellungen

Servername	BelkinSC
DHCP	Aktiviert
IP-Adresse	192.168.2.156
Netzmaske	255.255.255.0
Gateway	192.168.2.1
Seriennummer	xxxxxxxxx (siehe Geräteunterseite)
MAC-Adresse	xx:xx:xx:xx (siehe Geräteunterseite)
Version and Date (Version und Datum)	Aktuelle Versionsnummer und Datum der Firmware
Benutzername	admin
Kennwort	admin
Protokoll (seriell)	Telnet
Protokoll (Web)	HTTP
IP-Filter	Deaktivieren
Serielle Schnittstellen	
Baudrate	9600
Daten/Stopp	8-1
Parität	--
Flusskontrolle	--
Serielles Zeitlimit	0 Sekunden
Betriebsmodus	Konsolenserver
TCP-Schnittstelle	**Schnittstelle 1** 4001
	Schnittstelle 2 4002
	- - - - - - - -
	Schnittstelle 16 4016






F1D120ea (RJ45-Buchse–DB9-Buchse DTE)

DB9-Buchse/DTE-Adapter

Anwendungsbereiche: Bay Accelar, Nortel, usw.
Artikelnr.: F1D120ea: Einzelpack
F1D120ea8PK: 8er-Pack

Adapter		
Signal	RJ45	DB9-Buchse
DSR	1	4
DCD	6	
RTS	2	8
GND (Erde)	3	5
TxD	4	2
RxD	5	3
CTS	7	7
DTR	8	6 1 (DCD)




F1D121ea (RJ45-Buchse–DB25-Buchse DTE)

DB25-Buchse/DTE-Adapter

Anwendungsbereiche: DTE-Geräte wie PC
Artikelnr.: F1D121ea: Einzelpack

Adapter		
Signal	RJ45	DB25-Buchse
DSR	1	20
DCD	6	
RTS	2	5
GND (Erde)	3	7
TxD	4	3
RxD	5	2
CTS	7	4
DTR	8	6
		8 (DCD)



F1D122ea (RJ45-Buchse–DB25-Stecker DCE)

DB25-Stecker/DCE-Adapter

Anwendungsbereiche: Modems
Artikelnr.: F1D122ea: Einzelpack

Adapter		
Signal	RJ45	DB25-Stecker
DSR	1	6
RTS	2	4
GND (Erde)	3	5
TxD	4	2
RxD	5	3
DCD	6	1
CTS	7	5
DTR	8	20




F1D123ea (RJ45-Buchse–DB25-Stecker DTE)

DB25-Stecker/DTE-Adapter

Anwendungsbereiche: Sun SPARC, usw.
Artikelnr.: F1D123ea: Einzelpack

<table>
<tr><th colspan="3">Adapter</th></tr>
<tr><td>Signal</td><td>RJ45</td><td>DB25-Stecker</td></tr>
<tr><td>DSR</td><td>1</td><td rowspan="2">20</td></tr>
<tr><td>DCD</td><td>6</td></tr>
<tr><td>RTS</td><td>2</td><td>5</td></tr>
<tr><td>GND (Erde)</td><td>3</td><td>7</td></tr>
<tr><td>TxD</td><td>4</td><td>3</td></tr>
<tr><td>RxD</td><td>5</td><td>2</td></tr>
<tr><td>CTS</td><td>7</td><td>4</td></tr>
<tr><td>DTR</td><td>8</td><td>6</td></tr>
</table>





F1D124ea (RJ45-Buchse–RJ45-Stecker CISCO)

RJ45-Stecker-Adapter

Anwendungsbereiche: SUN-Geräte

Artikelnr.: F1D124ea: Einzelpack
F1D124ea8PK - 8er-Pack

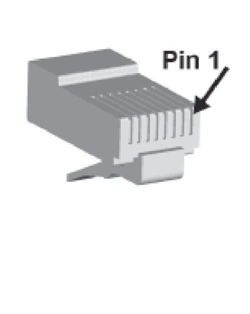
Adapter		
Signal	RJ45	RJ45-Stecker
DSR	1	2
RTS	2	8
GND (Erde)	3	4
		5
TxD	4	6
RxD	5	3
CTS	7	1
DTR	8	7






RJ45-Kontaktbelegung von Standard-Ethernet-Kabeln

Pin	Beschreibung
1	Tx+
2	Tx-
3	Rx+
4	NC
5	NC
6	Rx-
7	NC
8	NC








Schnittstellennummern werden in drei Kategorien eingeteilt: Bekannte Schnittstellen, registrierte Schnittstellen und dynamische bzw. private Schnittstellen. Bekannte Schnittstellen liegen im Bereich 0 bis 1023. Registrierte Schnittstellen liegen im Bereich 1024 und 49151. Dynamische bzw. private Schnittstellen befinden sich im Bereich 49152 bis 65535.

Bekannte Schnittstellen werden von der IANA zugewiesen und stehen auf den meisten Systemen nur Systemprozessen oder privilegierten Benutzern zur Verfügung. Die folgende Tabelle zeigt einige dieser bekannten Schnittstellennummern. Weitere Informationen finden Sie auf der Website der IANA: http://www.iana.org/assignments/port-numbers.

Portnummer	Protokoll	TCP/UDP
21	FTP (File Transfer Protocol)	TCP
22	SSH (Secure Shell)	TCP
23	Telnet	TCP
25	SMTP-Protokoll (Simple Mail Transfer Protocol)	TCP
37	Zeit	TCP, UDP
39	RLP (Resource Location Protocol)	UDP
49	TACACS, TACACS+	UDP
53	DNS	UDP
67	BOOTP Server	UDP
68	BOOTP Client	UDP
69	TFTP	UDP
70	Gopher	TCP
79	Finger	TCP
80	HTTP	TCP
110	POP3	TCP
119	NNTP (Network News Transfer Protocol)	TCP
161/162	SNMP	UDP
443	HTTPS	TCP






BOOTP (Bootstrap Protocol)

Entspricht DHCP, ist jedoch für kleinere Netze gedacht. Weist die IP-Adresse für eine bestimmte Dauer automatisch zu.

CHAP (Challenge Handshake Authentication Protocol)

Sicheres Protokoll für Verbindungen mit einem System; CHAP ist sicherer als PAP.

DHCP (Dynamic Host Configuration Protocol)

Internet-Protokoll zur automatischen Konfiguration von Computern in TCP/IP-Netzwerken.

DNS (Domain Name Server)

System, mit dem ein Netzwerk-Namensserver Hostnamen zu numerischen IP-Adressen auflösen kann.

Kerberos

Netzwerk-Authentifizierungsprotokoll, das eine starke Authentifizierung für Client/Server-Anwendungen über eine geheime Verschlüsselung ermöglicht.

LDAP (Lightweight Directory Access Protocol)

Protokoll für den Zugriff auf Verzeichnisinformationen.



NAT: Network Address Translation (Netzwerkadressenübersetzung)

Internet-Standard, mit dem ein LAN eine Reihe von IP-Adressen für den internen und eine zweite Reihe für den externen Datenverkehr nutzen kann. Dadurch können Unternehmen ihre internen Netzwerke vom öffentlichen Internet abschirmen.

NFS (Network File System)

Protokoll zur gemeinsamen Nutzung von Dateien in einem Netzwerk. Benutzer können Dateien auf einem entfernten Computer anzeigen, speichern, und aktualisieren. Mit NFS können Sie ein Dateisystem ganz oder teilweise einhängen. Benutzer können auf die eingehängten Teilsysteme mit denselben Rechten wie beim Benutzerzugriff auf die einzelnen Dateien zugreifen.

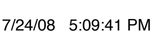
NIS (Network Information System)

Von Sun Microsystems entwickeltes System zur Verbreitung von Systemdaten wie Benutzer- und Hostnamen in einem Computernetzwerk.

NMS (Network Management System)

NMS dient als zentraler Server, der SNMP-Informationen mittels SNMP von den Computern abruft und entgegennimmt.







NTP-Protokoll (Network Time Protocol)
Protokoll zur Synchronisierung der Zeit auf vernetzten Computern und Geräten.

PAP-Protokoll (Password Authentication Protocol)
Methode zur Authentifizierung von Benutzern, bei der Benutzername und Kennwort über ein Netzwerk übertragen und mit einer Namen/Kennwort-Paartabelle verglichen werden.

PPP-Protokoll (Point-to-Point Protocol)
Protokoll zur Erstellung und Ausführung von IP- und weiteren Netzwerkprotokollen über eine serielle Verbindung.

RADIUS (Remote Authentication Dial-In User Service)
Authentifizierungs- und Buchungsprotokoll. Ermöglicht Fernzugriffsservern die Kommunikation mit einem zentralen Server zur Authentifizierung von DFÜ-Benutzern und ihrer Zugriffsberechtigungen. Ein Unternehmen speichert Benutzerprofile in einer zentralen Datenbank, die alle entfernten Server gemeinsam nutzen können.

SNMP-Protokoll (Simple Network Management Protocol)
Protokoll, mit dem Systemadministratoren Netzwerke und angeschlossene Geräte überwachen und auf Anforderungen aus anderen Netzwerk-Hosts reagieren können.



SMTP-Protokoll (Simple Mail Transfer Protocol)
TCP/IP-Protokoll zum Austausch von E-Mails zwischen Servern.

SSL (Secure Sockets Layer)
Protokoll zur Authentifizierung und Verschlüsselung von Daten zwischen einem Webserver und einem Browser.

SSH (Secure Shell)
Sicheres Übertragungsprotokoll auf Basis einer Verschlüsselung mit öffentlichen Schlüsseln.

TACACS+ (Terminal Access Controller Access Control System)
Authentifizierungsmethode in UNIX-Netzwerken. Sie ermöglicht einem entfernten Zugriffsserver die Kommunikation mit einem Authentifizierungsserver um festzustellen, ob der Benutzer Zugriff auf das Netzwerk hat.

Telnet
Terminal-Protokoll, das eine benutzerfreundliche Methode zum Aufbau von Terminalverbindungen zu einem Netzwerk-Host bietet.





Der Konsolenserver unterstützt eine sichere Webseitenkonfiguration (auch als https bezeichnet). Für die serverseitige Authentifizierung stehen zwei Arten von Zertifikatdateien zur Verfügung.

- Eigensignatur: Benutzer können die Zertifikatdateien selbst erstellen. Der Schwachpunkt liegt darin, dass der Client zur Annahme eines Zertifikats aufgefordert wird, das von einer dem Browser unbekannten Autorität signiert ist. In der Regel muss der Client-Browser das Zertifikat nur einmal annehmen und wird danach nicht mehr behelligt.
- Signatur durch eine Zertifizierungsstelle: Benutzer erstellen CA-Dateien und senden sie zur Signatur an eine Zertifizierungsstelle. Der Hauptvorteil liegt darin, dass der Client nicht zur Annahme eines Zertifikats aufgefordert wird.

Die Benutzer müssen das openSSL-Toolkit installieren, bevor sie solche CA-Dateien erstellen können. Im Folgenden wird erläutert, wie Sie das Zertifikat für den Webserver des Konsolenservers über openSSL und die Linux-Shell generieren. Das openSSL-Toolkit können Sie von folgender Website herunterladen: http://www.openssl.org/.

1. Eigensigniertes CA:

    i) Erstellen Sie einen Schlüssel und ein X.509-Zertifikat:





Linux-Befehlszeile:

openssl req -x509 -newkey rsa:1024 -days 1024 -keyout cakey.pem -out cacert.pem

Hier können folgende Optionen geändert werden:

* der PK-Algorithmus kann von RSA zu DSA geändert werden, ebenso die Bitlänge des Schlüssels (512, 1024, 2048, 4096).

* Gültigkeitsdauer des Zertifikats; wir haben 1024, also knapp 3 Jahre, festgelegt.

Sie können auch ein Start- und ein Enddatum für die Gültigkeit des Zertifikats festlegen. Sie werden zweimal zur Eingabe der PEM-Passphrase für den Schlüssel aufgefordert. Danach müssen Sie einige Informationen für das Zertifikat eingeben:

Beispiel für eine Eingabeaufforderung:

Land	<US>
Staat oder Bundesland	<IhrLand>
Ort	<Anchorage>
Firma	<Name Ihres Unternehmens>
Prolix Organizational Unit	Forschung & Entwicklung
Eigenname (Hostname des Servers)	<IPCS>
E-Mail-Adresse des Server-Administrators	<Sie@IhreDomäne.dom>





ii) Passphrase aufschlüsseln:

openssl rsa -in cakey.pem -out cakey-nopassword.pem

iii) Schlüssel- und X.509-Zertifikatdateien in server.pem aufnehmen:

cat cakey-nopassword.pem cacert.pem > server.pem

iv) Alle 3 PEM-Dateien aufnehmen und auf den IPCS-Server hochladen:

server.pem , cacert.pem , cakey.pem

2. Signatur durch vertrauenswürdige Zertifizierungsstelle:

i) Privaten Schlüssel **cakey.pem vorbereiten:**

openssl genrsa –des3 –out cakey.pem 1024

Bedeutung der Parameter:

genrsa : privaten RSA-Schlüssel generieren

des3 : Zertifikat mit DES3 verschlüsseln

1024: Schlüsselgröße: 1024 Bit



ii) Zertifikat-Signaturantrag ausstellen:

openssl req –new –key cakey.pem –out server.csr

Das openSSL-Toolkit gibt dem Benutzer in einer Meldung eine Ausfüllhilfe für das Registrierungsformular an die Hand. Das ausgefüllte Formular können die Benutzer als CSR-Datei zu Testzwecken an www.verisign.com senden oder zur Beantragung eines signierten Zertifikats an http://www.hitrust.com.tw/hitrustexe/frontend/default_tw.asp (nach Taiwan) senden. Benennen Sie die erhaltene Zertifikatdatei in „cacert.pem" um.

iii) Passphrase aufschlüsseln:

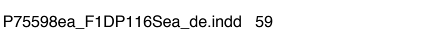
openssl rsa –in cakey.pem –out cakey-nopassword.pem

iv) Schlüssel- und X.509-Zertifikatdateien in server.pem aufnehmen:

cat cakey-nopassword.pem cacert.pem > server.pem

v) Alle 3 PEM-Dateien für den Upload bereitstellen:

server.pem , cacert.pem , cakey.pem





FCC-Erklärung

ERKLÄRUNG DER KONFORMITÄT MIT DEN VORSCHRIFTEN FÜR DIE ELEKTROMAGNETISCHE VERTRÄGLICHKEIT

Wir, Belkin International, Inc., 501 West Walnut Street, Compton, CA 90220, USA, erklären hiermit alleinverantwortlich, dass der Artikel
F1DP116S, auf den sich diese Erklärung bezieht,

in Einklang mit Teil 15 der FCC-Bestimmungen steht. Der Betrieb unterliegt den beiden folgenden Bedingungen:

(1) Dieses Gerät darf schädigende Störungen nicht verursachen, und (2) dieses Gerät muss jedwede Störung annehmen, einschließlich der Störungen, die einen unerwünschten Betrieb verursachen könnten.

Dieses Gerät entspricht nachweislich den Grenzwerten für digitale Geräte der Klasse A gemäß Teil 15 der FCC-Bestimmungen. Diese Grenzwerte sollten einen vernünftigen Schutz vor schädlicher Interferenz liefern, wenn das Gerät in einer gewerblichen Umgebung betrieben wird. Durch dieses Gerät wird hochfrequente Energie erzeugt, genutzt und unter Umständen abgestrahlt, und es kann daher bei nicht vorschriftsmäßiger Installation und Nutzung Funkstörungen verursachen. Der Betrieb dieses Geräts in Wohngebieten kann wahrscheinlich schädliche Interferenz verursachen; in diesem Fall muss der Benutzer die Interferenz auf eigene Kosten beseitigen.



Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Réglement sur le brouillage radioélectrique édicté par le Ministére des Communications du Canada.

CE-Konformitätserklärung

Wir, Belkin International, Inc., erklären hiermit in alleiniger Verantwortung, dass der Artikel F1DP116S, auf den sich diese Erklärung bezieht, in Einklang mit der Fachgrundnorm Störaussendung EN55022 Klasse A und der Fachgrundnorm Störfestigkeit EN55024 sowie LVP EN61000-3-2 und EN61000-3-3 steht.

ICES-Erklärung

Dieses Digitalgerät der Klasse A entspricht der kanadischen Richtlinie ICES-003. Cet appareil numérique de la classe A est conforme á la norme NMB-003 du Canada.

Zwei Jahre beschränkte Herstellergarantie von Belkin International, Inc.

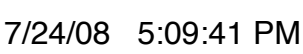
Garantieleistung.

Belkin International, Inc. („Belkin") garantiert dem ursprünglichen Käufer dieses Belkin-Produkts, dass dieses Produkt frei von Material-, Verarbeitungs-, und Konstruktionsfehlern ist.

Garantiedauer.

Belkin gewährt für dieses Belkin-Produkt eine zweijährige Garantie.







Problembehebung.
Herstellergarantie.
Belkin wird das Produkt nach eigenem Ermessen entweder kostenlos (abgesehen von den Versandkosten) reparieren oder austauschen.

Garantieausschluss.
Alle oben genannten Garantien verlieren ihre Gültigkeit, wenn das Belkin-Produkt Belkin auf Anfrage nicht auf Kosten des Käufers zur Überprüfung zur Verfügung gestellt wird oder wenn Belkin feststellt, dass das Belkin-Produkt nicht ordnungsgemäß installiert worden ist, und dass unerlaubte Änderungen daran vorgenommen worden sind. Die Herstellergarantie von Belkin gilt nicht für (Natur)gewalten wie Überschwemmungen, Erdbeben und Blitzschlag sowie Krieg, Vandalismus, Diebstahl, normalen Verschleiß, Erosion, Wertminderung, Veralterung, schlechte Behandlung, Beschädigung durch Störungen aufgrund von Unterspannung (z. B. Spannungsabfall oder -Senkung) oder nicht erlaubte Programm- oder Systemänderungen

Service.
Um Unterstützung von Belkin zu bekommen, gehen Sie nach folgenden Schritten vor:




1. Schreiben Sie an Belkin International, Inc., 501 W. Walnut St., Compton CA 90220, Attn: Customer Service oder wenden Sie sich innerhalb von 15 Tagen nach dem Vorfall telefonisch unter (800)-223-5546 an Belkin. Halten Sie die folgenden Informationen bereit:
    a. Die Artikelnummer des Belkin-Produkts.
    b. Wo Sie das Produkt erworben haben.
    c. Das Kaufdatum.
    d. Kopie der Originalquittung.

2. Die entsprechenden Mitarbeiter/innen informieren Sie darüber, wie Sie Ihre Rechnung und das Belkin-Produkt versenden müssen und wie Sie fortfahren müssen, um Ihre Ansprüche geltend zu machen.

Belkin behält sich vor, das beschädigte Belkin-Produkt zu überprüfen. Alle Kosten, die beim Versand des Belkin-Produkts an Belkin zum Zweck der Überprüfung entstehen, sind vollständig durch den Käufer zu tragen. Wenn Belkin nach eigenem Ermessen entscheidet, dass es nicht angebracht ist, das beschädigte Gerät an die Belkin zu schicken, kann Belkin nach eigenem Ermessen eine Reparaturstelle damit beauftragen, das Gerät zu überprüfen und einen Kostenvoranschlag für die Reparaturkosten des Gerätes zu machen. Die Kosten für den Versand zu einer solchen Reparaturstelle und die eventuellen Kosten für einen Kostenvoranschlag gehen vollständig zu Lasten des Käufers. Beschädigte Geräte müssen zur Überprüfung zur Verfügung stehen, bis das Reklamationsverfahren abgeschlossen ist. Wenn Ansprüche beglichen werden, behält sich Belkin das Recht vor, Ersatzansprüche an eine bestehende Versicherung des Käufers zu übertragen.





Garantiegesetze.

DIESE GARANTIE BILDET DIE ALLEINIGE GARANTIE VON BELKIN. ES GIBT KEINE ANDERE GARANTIE, EXPLIZIT ERWÄHNT ODER IMPLIZIT, AUSSER WENN DIES VOM GESETZ VORGESCHRIEBEN IST, EINSCHLIESSLICH DER IMPLIZITEN GARANTIE ODER DES QUALITÄTSZUSTANDS, DER ALLGEMEINEN GEBRAUCHSTAUGLICHKEIT ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, UND SOLCHE IMPLIZITEN GARANTIEN, WENN ES SOLCHE GIBT, BEZIEHEN SICH AUSSCHLIESSLICH AUF DIE DAUER, DIE IN DIESER GARANTIE ZUGRUNDE GELEGT WIRD.

In manchen Ländern sind Einschränkungen bezüglich der Dauer der Garantie nicht zulässig. Die oben erwähnten Einschränkungen treffen für Sie dementsprechend nicht zu.

UNTER KEINEN UMSTÄNDEN HAFTET BELKIN FÜR ZUFÄLLIGEN, BESONDEREN, DIREKTEN, INDIREKTEN, MEHRFACHEN SCHADEN ODER FOLGESCHÄDEN WIE, ABER NICHT AUSSCHLIESSLICH, ENTGANGENES GESCHÄFT ODER PROFITE, DIE IHNEN DURCH DEN VERKAUF ODER DIE BENUTZUNG VON EINEM BELKIN-PRODUKT ENTGANGEN SIND, AUCH WENN SIE AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN AUFMERKSAM GEMACHT WORDEN SIND.



Diese Garantie räumt Ihnen spezifische Rechte ein, die von Land zu Land unterschiedlich ausgestaltet sein können. Da in manchen Ländern der Ausschluss oder die Beschränkung der Haftung für durch Zufall eingetretene oder Folgeschäden nicht zulässig ist, haben die vorstehenden Beschränkungen und Ausschlussregelungen für Sie möglicherweise keine Gültigkeit.







63



BELKIN®

Serieller OmniView® Konsolenserver

Kostenloser technischer Support*

Technische Informationen und Unterstützung erhalten Sie unter www.belkin.com im Bereich technischer Support. Wenn Sie den technischen Support telefonisch erreichen wollen, wählen Sie die entsprechende Nummer auf der unten aufgeführten Liste*.

*Zum Ortstarif

Land	Nummer	Internet-Adresse
ÖSTERREICH	0820 200766	http://www.belkin.com/uk/support/
BELGIEN	07 07 00 073	http://www.belkin.com/nl/support/
TSCHECHISCHE REPUBLIK	239 000 406	http://www.belkin.com/uk/support/
DÄNEMARK	701 22 403	http://www.belkin.com/uk/support/
FINNLAND	00800 - 22 35 54 60	http://www.belkin.com/uk/support/
FRANKREICH	08 - 25 54 00 26	http://www.belkin.com/fr/support/
DEUTSCHLAND	0180 - 500 57 09	http://www.belkin.com/de/support/
GRIECHENLAND	00800 - 44 14 23 90	http://www.belkin.com/uk/support/
UNGARN	06 - 17 77 49 06	http://www.belkin.com/uk/support/
ISLAND	800 8534	http://www.belkin.com/uk/support/
IRLAND	0818 55 50 06	http://www.belkin.com/uk/support/
ITALIEN	02 - 69 43 02 51	http://www.belkin.com/it/support
LUXEMBURG	34 20 80 85 60	http://www.belkin.com/uk/support/
NIEDERLANDE	0900 - 040 07 90 0,10 € pro Minute	http://www.belkin.com/nl/support/
NORWEGEN	81 50 0287	http://www.belkin.com/uk/support/
POLEN	00800 - 441 17 37	http://www.belkin.com/uk/support/
PORTUGAL	707 200 676	http://www.belkin.com/uk/support/
RUSSLAND	495 580 9541	http://www.belkin.com/uk/support/
SÜDAFRIKA	0800 - 99 15 21	http://www.belkin.com/uk/support/
SPANIEN	902 - 02 43 66	http://www.belkin.com/es/support/
SCHWEDEN	07 - 71 40 04 53	http://www.belkin.com/uk/support/
SCHWEIZ	08 - 48 00 02 19	http://www.belkin.com/uk/support/
GROSSBRITANNIEN	0845 - 607 77 87	http://www.belkin.com/uk/support/
SONSTIGE LÄNDER	+44 - 1933 35 20 00	




BELKIN®

www.belkin.com

Belkin Ltd.
Express Business Park
Shipton Way, Rushden
NN10 6GL, Großbritannien

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk
Niederlande

Belkin GmbH
Hanebergstraße 2
80637 München
Deutschland

Belkin SAS
130 rue de Silly
92100 Boulogne Billancourt
Frankreich

Belkin Iberia
Avda. Cerro del Aguila 3
28700 San Sebastián de los Reyes
Spanien

Belkin Schweden
Knarrarnäsgatan 7
164 40 Kista
Schweden

P75598ea

